構築ガイド

Lync リバースプロキシ

AX/Thunder シリーズ構築ガイド

Document No. : DG_AXTH_201309 Ver.1.0
Date : 2013/9/30

A10 ネットワークス株式会社
東京都港区虎ノ門 4-3-20 神谷町 MT ビル 16 階
TEL 03-5777-1995 / FAX 03-5777-1997
E-Mail jinfo@a10networks.com

目次

1　概要

リバースプロキシは、主にインターネット経由でアクセスしてくる外部の Lync ユーザーに対して、Lync の Web サービスを利用した機能提供並びに Web 会議時の Office Web Apps を利用したパワーポイント資料の共有に利用されます。また、Lync モバイルクライアントが Lync サーバーとやり取りするメッセージは、基本的に全て Web サービス経由となり、外部からの接続は常にリバースプロキシ経由での通信となるため、リバースプロキシは大変重要な役割を持っているといえます。

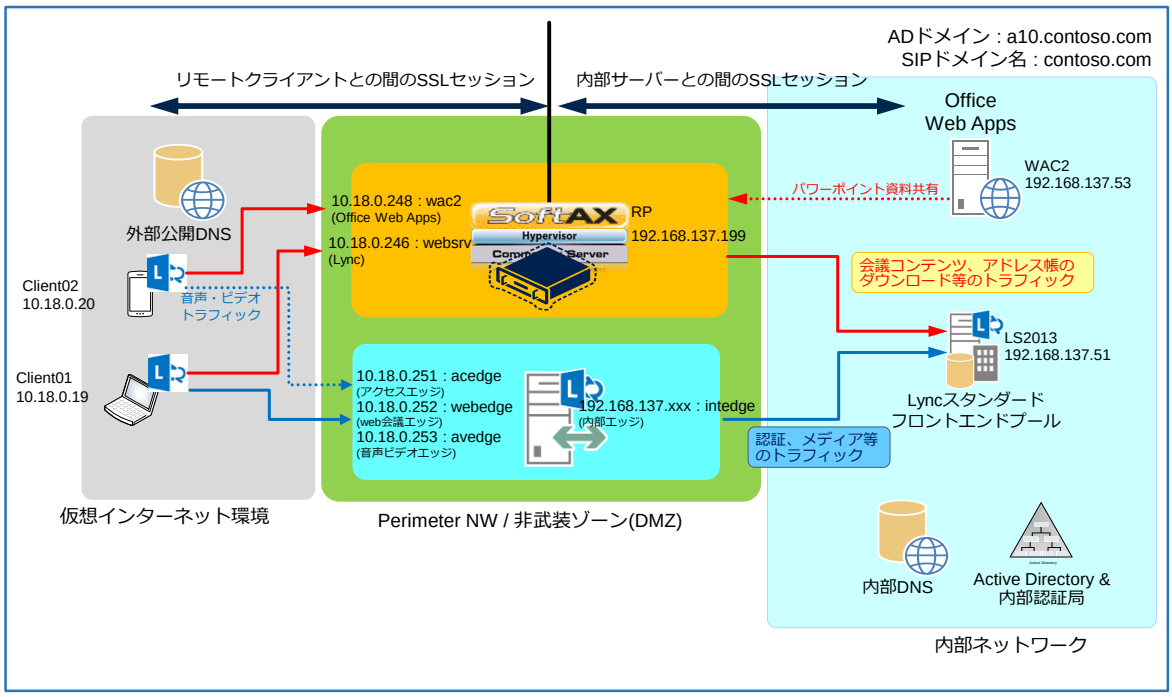
本書では、A10 ネットワークス社の AX/Thunder シリーズでリバースプロキシを構成する方法について説明します。

注意 ： リバースプロキシには、マイクロソフト社製 TMG (Threat Management Gateway)が主に利用されていましたが、同製品は 2012/11/30 に販売終了となっており、現時点でマイクロソフト社からは代替製品の販売も行われていません。

2　システム構成

本書のシナリオで使用している環境は、以下の通りとなります。

- SoftAX　2.7.1-P2, build 57
- Windows Server 2008 R2 (Hyper-V プラットフォーム)
- Lync Server 2013 Standard Edition CU2　(Windows Server 2008 R2)
- Lync Mobile 2013 for iPad 5.1
- Lync 2013 CU2 (Windows 7 Enterprise Edition)
- Office Web Apps サーバー (Windows Server 2008 R2)



Lync 外部接続に必要なリバースプロキシ機能を SoftAX で代替し、リモートクライアント(社外ユーザーが利用)と内部の Lync フロントエンドサーバー、Office Web Apps サーバー間の SSL セッションを SoftAX で分断し、中継します。

SoftAX は、社外からアクセスしてくる Lync クライアントや Lync モバイルクライアントからの通信を、Lync フロントエンドサーバーや Office Web Apps サーバーとして終端し、内部の Lync フロントエンドサーバーや Office Web Apps サーバーに対しては新たにセッションを確立し、社外からの通信を中継します。

メモ：
Lync フロントエンドサーバー：Lync のコアとなるサーバーの役割で、多くの機能を実行しています。
http:/technet.microsoft.com/ja-jp/library/gg398536.aspx
Office Web Apps サーバー：Lync 向けにパワーポイントファイルの共有をサポートします。
http://technet.microsoft.com/ja-jp/library/jj204792.aspx

SoftAX でリバースプロキシを展開することで、Lync リモートクライアントや Lync モバイルは、Lync フロントエンドサーバーの Web サービスから、アドレス帳や会議資料のダウンロード並びに会議参加/スケジュール URL へのアクセスができるようになります。

メモ：

SoftAX とは、A10 ネットワークス社のソフトウェアベースの仮想化サーバー負荷分散装置のことで、本書の環境では Windows Server 2008R2 の Hyper-V 上で動作しています。A10 ネットワークス社の負荷分散装置は、ソフトウェア版の SoftAX でも、ハードウェア製品とほぼ同等の機能を提供可能です。お客様は、自社の利用規模に合わせて最適な製品をお選びいただくことができます。

3　システム構築の事前作業

リバースプロキシとして SoftAX を構成するにあたり、以下の事前準備が必要となります。

- SoftAX 内部ネットワークインターフェース、外部ネットワークインターフェース向け IP アドレスの準備

  注意： 外部ネットワークインターフェース向けに割り当てる IP アドレスは、Lync, Office Web Apps の外部公開用 IP アドレスと同じサブネットが望ましく、通常であれば公開用 IP アドレスを一つ余分に準備する必要があります。昨今の IP アドレス(v4)の枯渇により、十分な数の IP アドレスを準備できないことも想定されますので、この問題を解決するための方法を、後述の本検証環境構成において説明します。

- Lync フロントエンドサーバー、Office Web Apps サーバーの外部公開 URL(Web サーバー)の FQDN に割り当てる外部公開用 IP アドレスの準備
- 外部公開用 IP アドレスと紐づく FQDN の公開 DNS への登録
  - ✧ Lync トポロジービルダーで構成した、Lync フロントエンドサーバー、Office Web Apps サーバーの外部公開 URL(Web サーバー)の FQDN を公開 DNS へ登録
- 外部の商用認証局(CA)から発行されたサーバー証明書と秘密鍵の準備
  - ※ 本書の構成では商用証明局から発行された証明書ではなく、テスト用に作成した認証局の証明書を利用します。

メモ：

外部ユーザー向けに利用する証明書には、以下の FQDN もしくはワイルドカードを SAN(サブジェクト代替名)に含むサーバー証明書が必要となります。

Lync サーバーの公開 FQDN
Meet.<SIP ドメイン>
Dialin.<SIP ドメイン>
Lyncdiscover.<SIP ドメイン>
Office Web Apps 公開 FQDN
(Lync とは別に個別で証明書を作成する方法もあります)

証明書は外部ユーザーからのアクセス向けに利用するため、商用認証局から発行されるものが推奨されます。商用認証局から証明書を取得する方法は、ご利用される証明書発行機関までお問い合わせください。

4　システム構築手順概要

SoftAX でリバースプロキシ機能を展開するための手順は以下の通りです。

- 外部公開 Web サーバー証明書要求ファイル(CSR)の作成
  - ・SoftAX では SAN を含んだ CSR を作成できないため、ここでは Windows PC の証明書メニューから、必要な CSR ファイルを作成します。この他 OpenSSL 等のツールを利用しても作成は可能です。

- 証明書の発行・取得
  - ・本書のシナリオでは、社内認証局(CA)とは別の Windows 2008R2 認証局(CA)を利用して Web サーバー証明書の発行をしています。

- 社内ルート証明書
  - ・社内認証局(CA)のルート証明書をエクスポートします。

- SoftAX のネットワークを構成
  - ・既存ネットワーク構成に合わせ、内部・外部ネットワークインターフェース向け IP アドレス、デフォルトゲートウェイ、VLAN 等を構成します。

- リバースプロキシ機能を構成
  - ・Lync フロントエンドサーバー、Office Web Apps サーバー向け外部公開 Web サーバー証明書と社内認証局(CA)ルート証明書をインポートします。
  - ・サーバーSSL テンプレートを新規に作成し、先にインポートした社内 CA 証明書を割り当てます。
  - ・クライアント SSL テンプレートを新規に作成し、先に発行した外部公開 Web サーバー証明書と秘密鍵を割り当てます。(Lync と Office Web Apps 向けの公開証明書が別々の場合には、クライアント SSL テンプレートを各々に対して作成し、適切な証明書を割り当てる必要があります)
  - ・ソース IP パーシステンスのテンプレートを作成します。

・IP ソース NAT を作成し、変換先 IP アドレスとして SoftAX に定義した内部用ネットワークインターフェース IP アドレスを設定します。

注意 : Lync フロントエンドサーバー、Office Web Apps サーバーからの返信先 IP アドレスを、明示的に SoftAX の内部ネットワークインターフェースに割当てた IP アドレスにする必要性が無い場合(外部からのアクセスに対する返信を SoftAX の内部インターフェース向けにルーティングすることが可能なケース)、IP ソース NAT を構成する必要はありません。

・Lync フロントエンドサーバー、Office Web Apps サーバーの IP アドレスと通信ポート(4443、443)を、サーバとして定義します。
・Lync フロントエンドサーバー、Office Web Apps サーバー向けに各々サービスグループを定義して、先に構成したサーバを割り当てます。
・バーチャルサーバとして、Lync フロントエンドサーバー、Office Web Apps サーバーを定義し、各々に外部公開用 IP アドレスを設定します。
続いて、バーチャルサーバポートの設定で以下の様に構成情報を定義します。

- タイプ : https
- ポート : 443
- アドレス : 公開 FQDN に紐づく IP アドレス
  (クライアント向けインターフェース)
- ソース NAT プールの選択
- クライアント SSL テンプレートの選択
- サーバーSSL テンプレートの選択
- パーシステンステンプレートタイプで、ソース IP パーシステンスを選択
- ソース IP パーシステンスで適切なもの(先ほど定義したもの)を選択

5　証明書の準備

5.1　外部公開 Web サーバー証明書要求ファイル(CSR)の準備

Lync フロントエンドサーバー外部公開 URL 向けの Web サーバー証明書(SSL サーバー証明書とも言います) を取得するため、要求ファイル(CSR)を Windows の証明書メニューを利用して作成する方法を以下に記します。
本書の構成では、Lync フロントエンドサーバー外部公開 URL 向け Web サーバー証明書と Office Web Apps サーバー外部公開 URL 向け Web サーバー証明書を各々個別に作成しています。

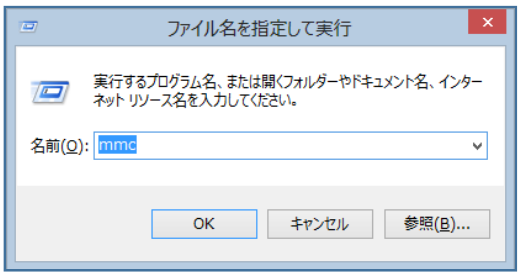
注意 : Lync エッジサーバー向けに作成する証明書で Lync フロントエンドサーバー外部公開 URL と Office Web Apps サーバー外部公開 URL の証明書も網羅する場合には、エッジサーバーの証明書要求ウィザードを利用することも可能です。この他、複数のサーバー役割(Lync フロントエンド、Office Web Apps)向けに一つの証明書を利用するケースや、SAN にワイルドカード証明書を利用するようなケースも考えられます。

CSR を作成する手順は幾つかの方法があり、こちらで示している手順はあくまで参考情報となります。AX/Thunder シリーズでも要求ファイルを作成するメニューはありますが、サブジェクト代替名(SAN)をサポートしていませんのでご注意ください。

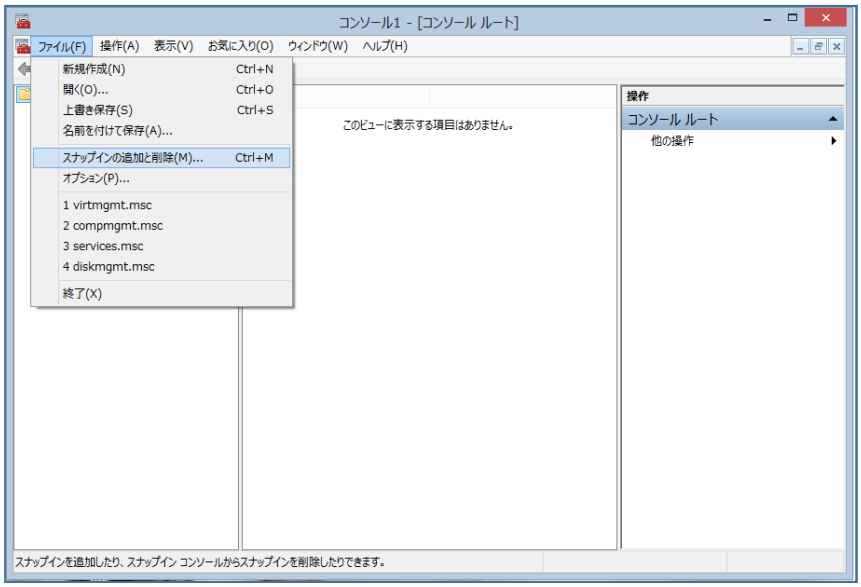
注意 : CSR ファイルの作成方法等については、各公開認証局で推奨方法が提示されている場合もありますので、事前に利用する公開認証局に確認してください。

Office Web Apps サーバー外部公開 URL 向けの Web サーバー証明書の要求・発行手順はこちらでは記載していませんが、証明書要求時の共通名、DNS 名のそれぞれに、Office Web Apps サーバー外部公開 URL の FQDN を指定することで、Lync フロントエンドサーバー外部公開 URL 向け Web サーバー証明書要求と同様の手順で証明書を作成できます。

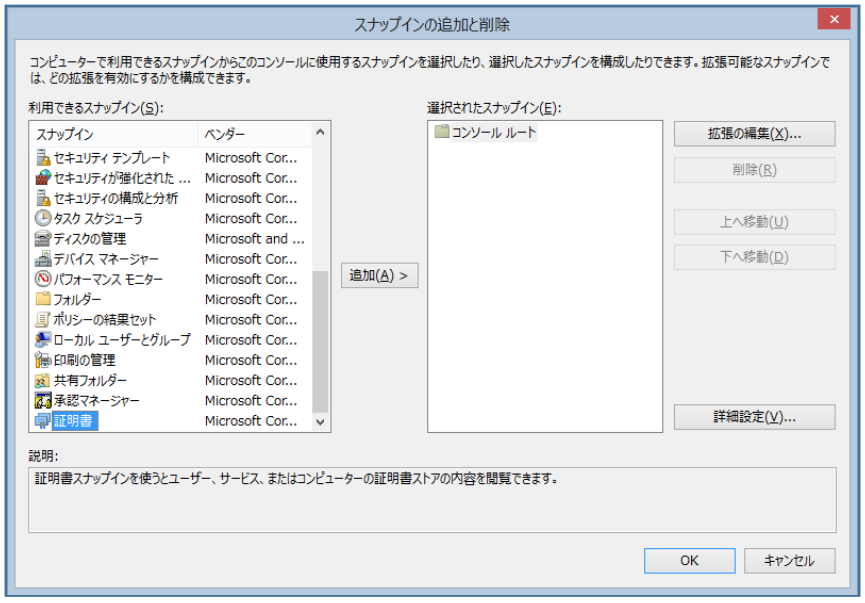
Windows PC 端末で、”ファイル名を指定して実行”で”mmc”と入力し”OK”をクリックします。



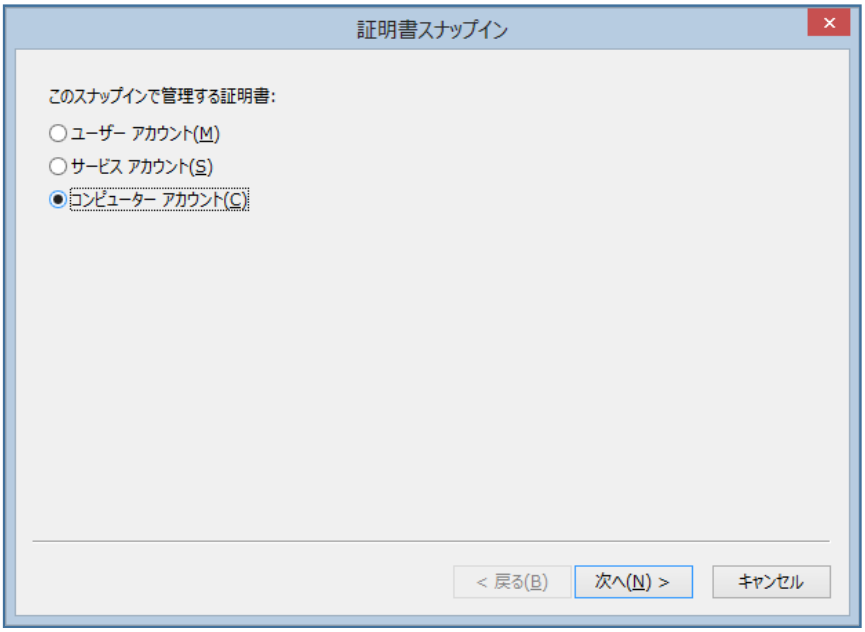
コンソールが立ち上がってくるので、”ファイル(F)” >> “スナップインの追加と削除 (M)…”を選択します。



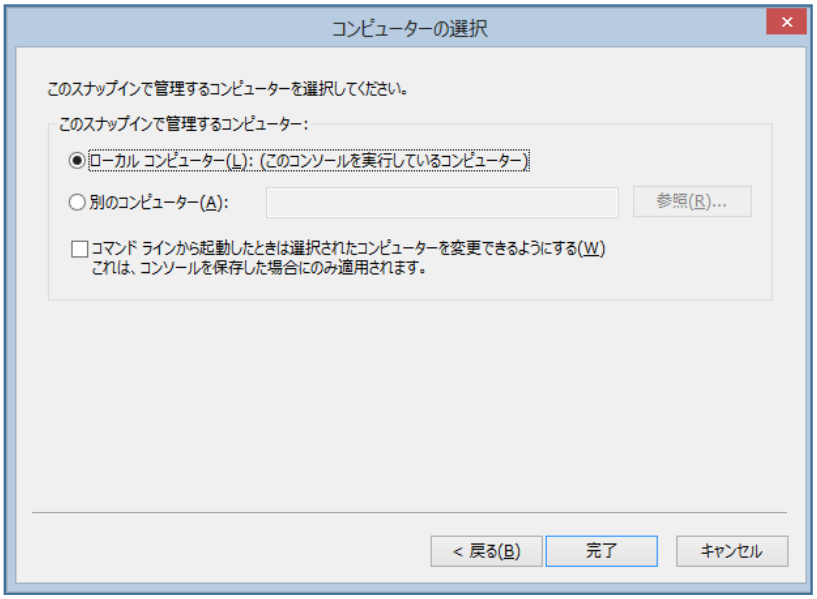
スナップインの追加と削除で、”利用できるスナップイン(S):”で”証明書”を選択し、”追加(A)>“をクリックします。



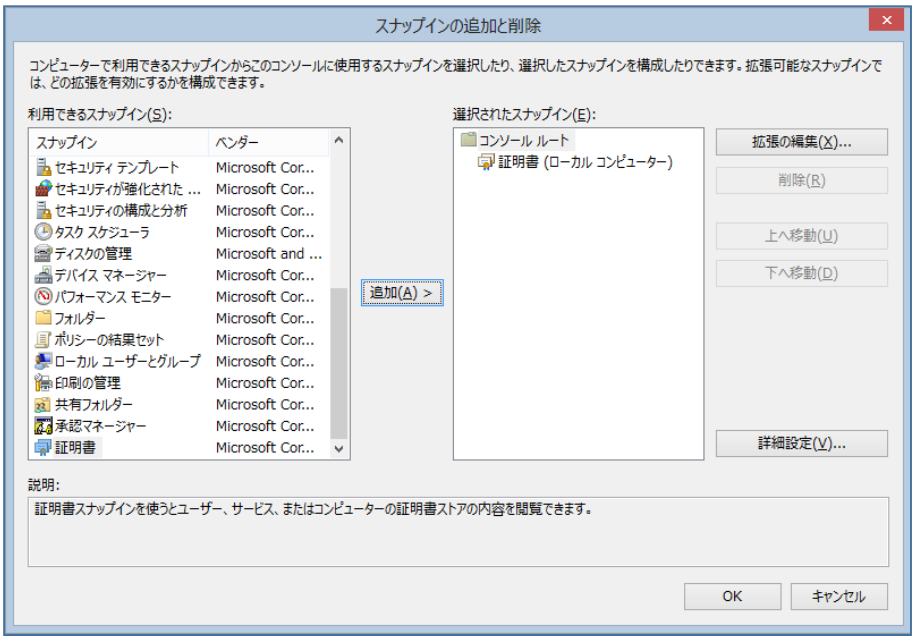
証明書スナップインのウィザードが開始するので、”このスナップインで管理する証明書:”で”コンピューターアカウント(C)”を選択し、”次へ(N)”をクリックします。



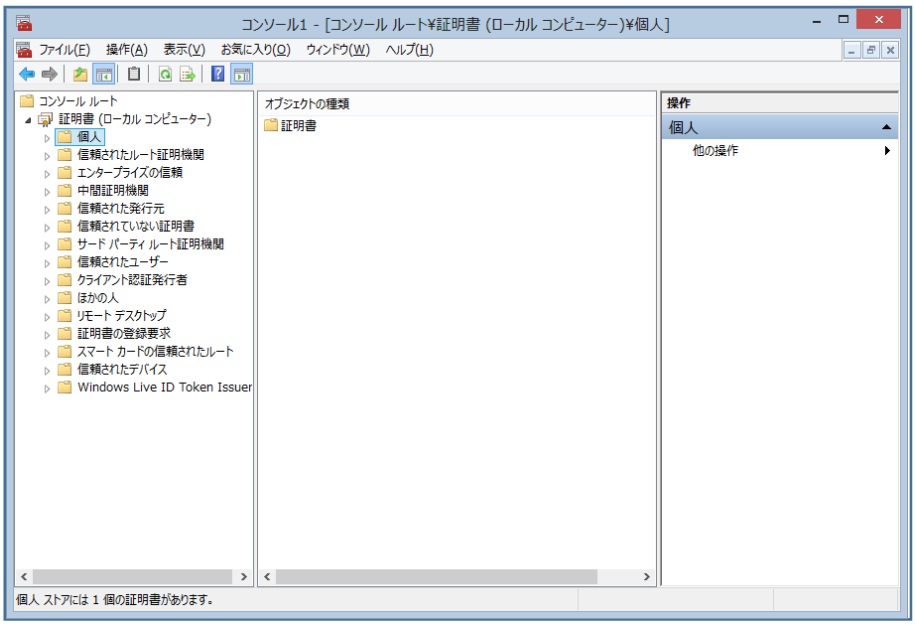
“このスナップインで管理するコンピューター:”で”ローカルコンピューター(L): (このコンソールを実行しているコンピューター)” を選択し完了ボタンをクリックします。



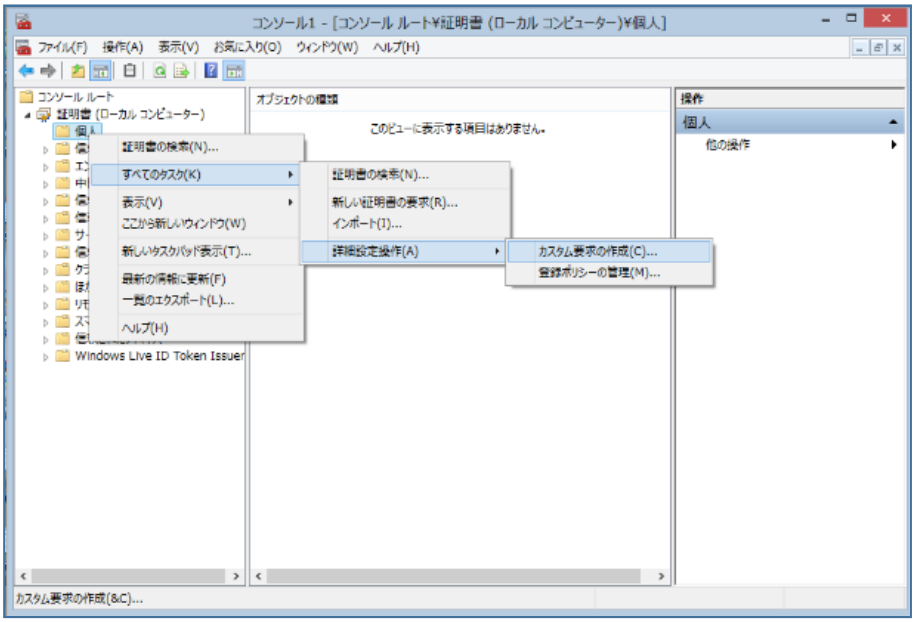
“選択されたスナップイン(E):に”証明書(ローカルコンピューター)”があることを確認し、”OK”をクリックして終了します。



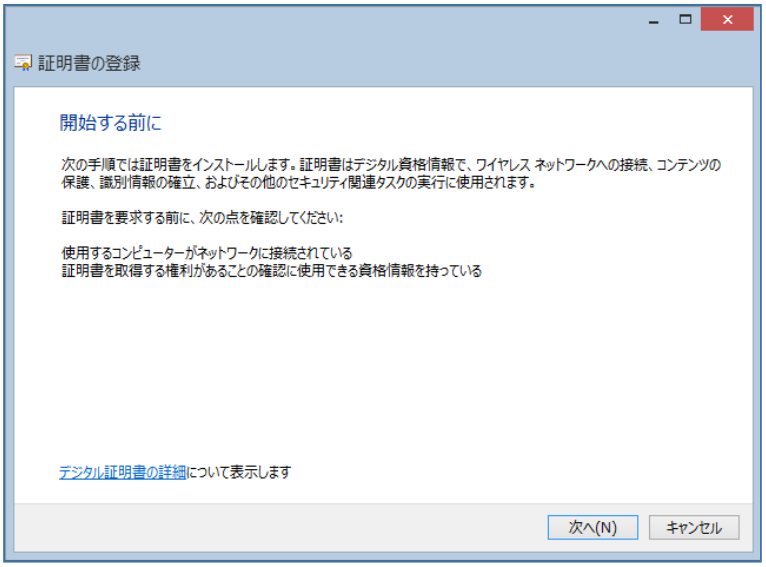
コンソールルート下の”証明書(ローカルコンピューター)”を展開します。



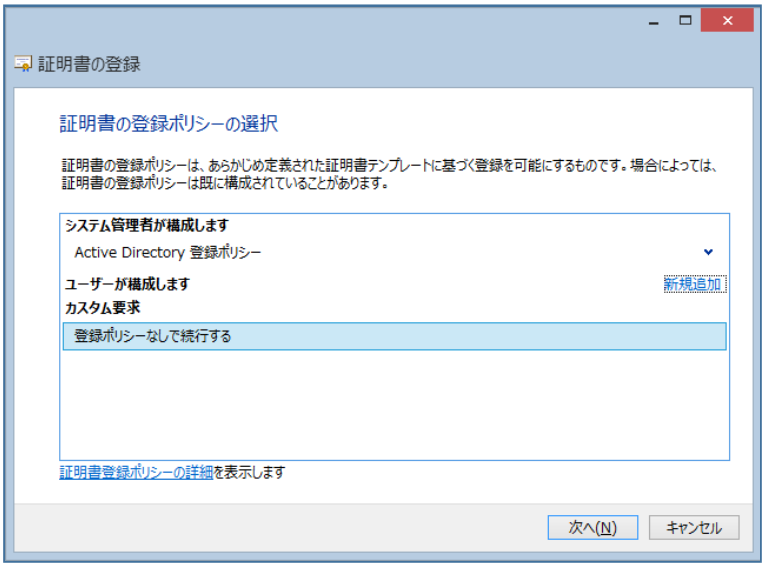
“個人”を右クリックし、”すべてのタスク(K)” >> “詳細設定操作(A) >> “カスタム要求の作成(C)”を選択します。



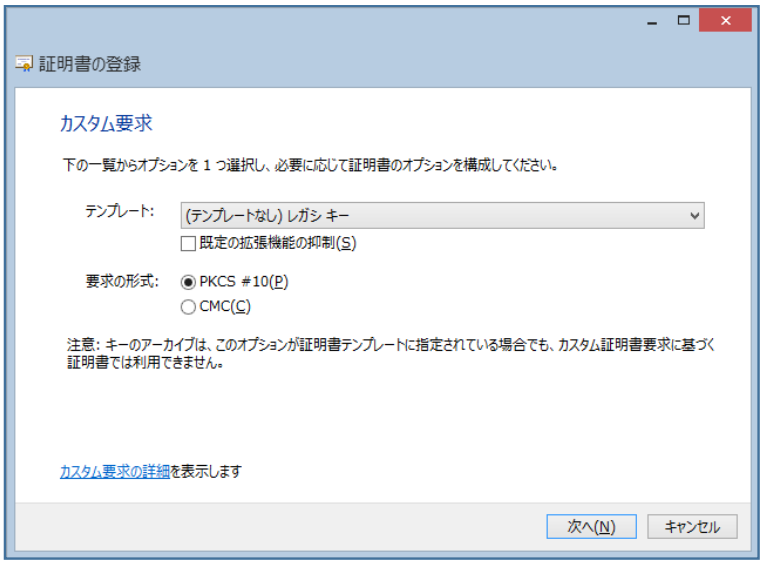
証明書の登録ウィザードが開始されます。



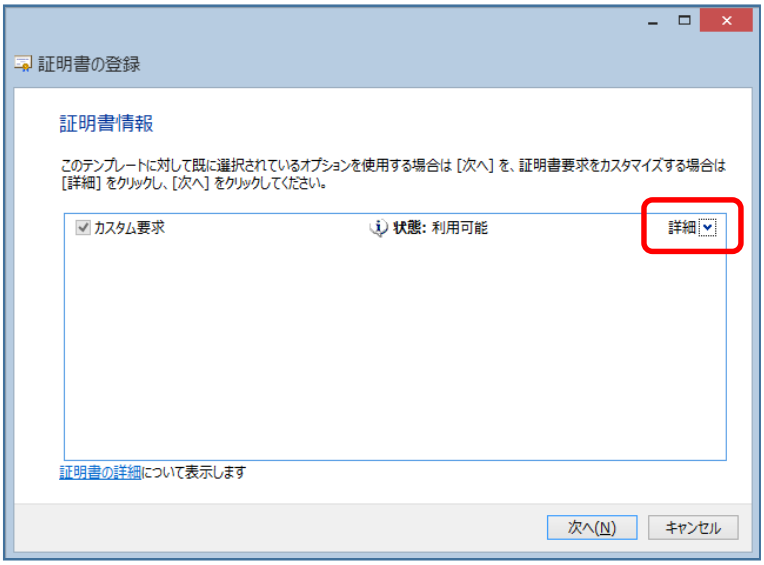
“証明書の登録ポリシーの選択”で”カスタム要求” >> “登録ポリシーなしで続行する”を選択し、”次へ(N)”をクリックします。



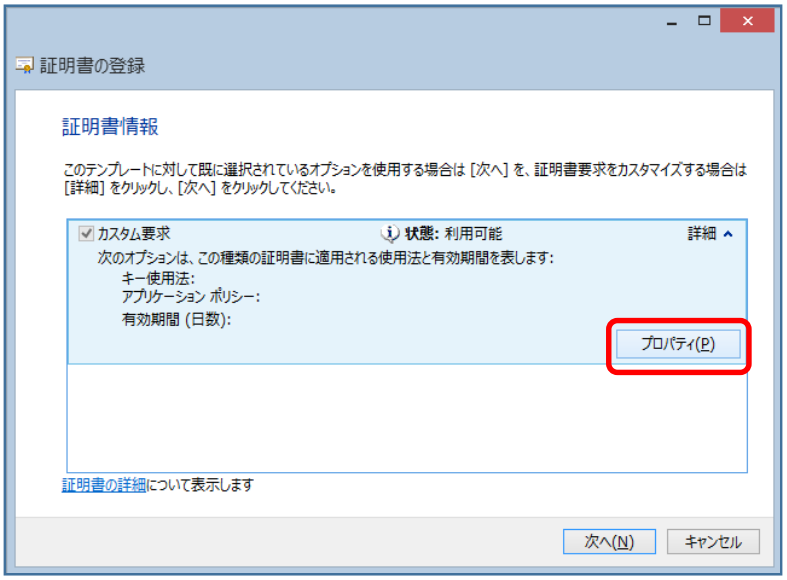
カスタム要求で、”テンプレート：(テンプレートなし)レガシーキー”、”要求形式：PKCS #10(P)”を選択し、”次へ(N)”をクリックします。



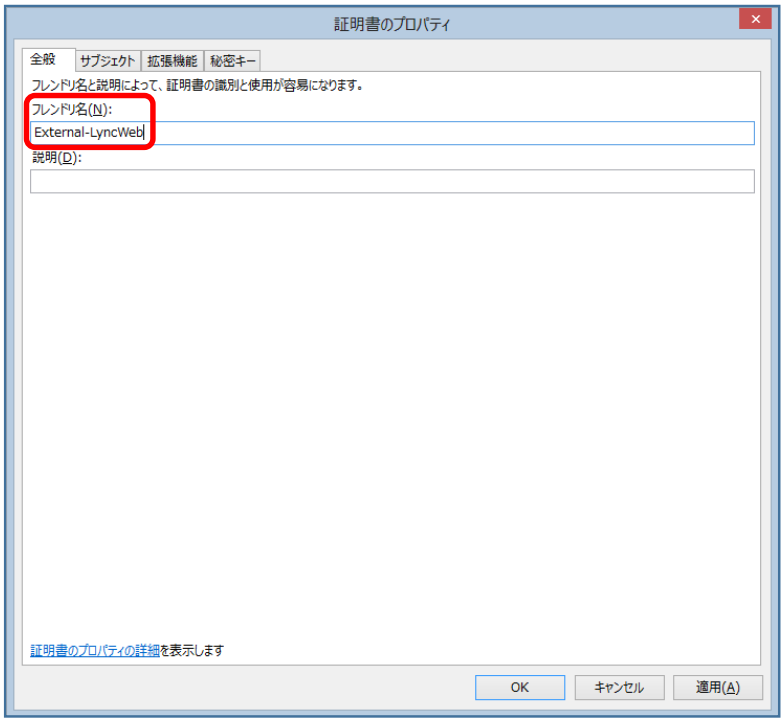
証明書要求をカスタマイズするため、”詳細”をクリックして展開します。



“プロパティ(P)”をクリックし、証明書のプロパティ画面を展開します。



全般タブの”フレンドリ名(N):”に適当な名前を入力します。



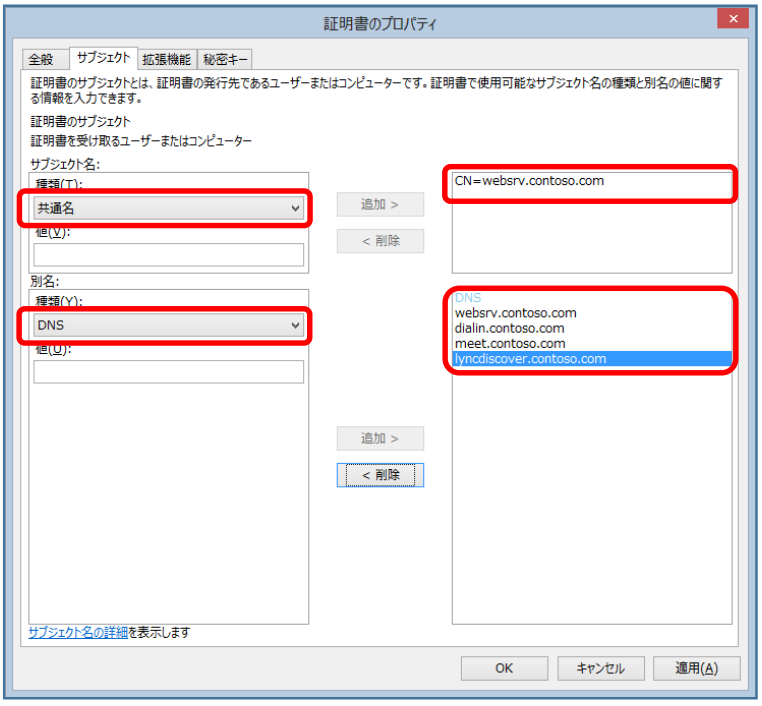
サブジェクトタブでサブジェクト名、サブジェクト代替名(別名)を定義します。

“サブジェクト”タブに移動し、”サブジェクト名”として”共通名”、”別名”(サブジェクト代替名)として”DNS”を選択し、適切なホスト名を登録していきます。

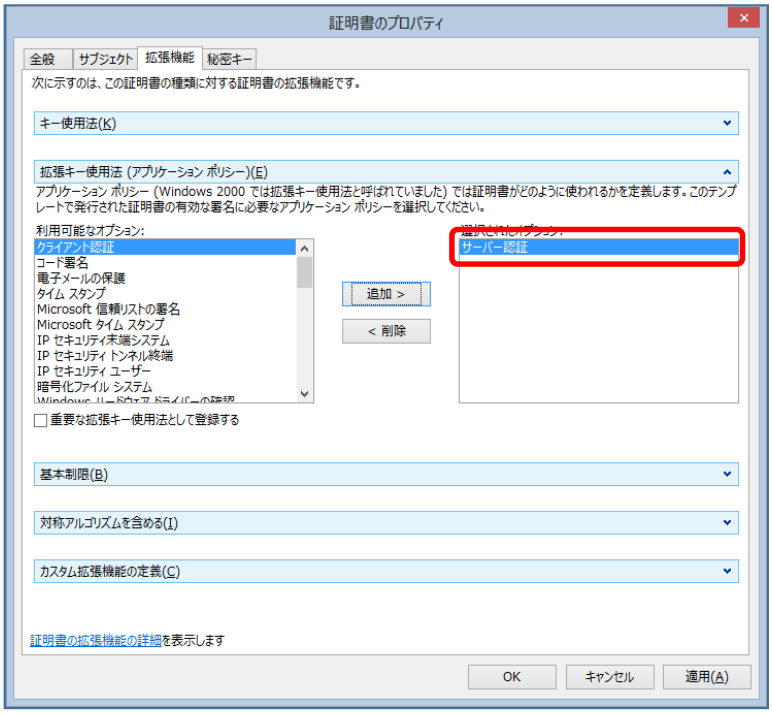
今回は、以下のホスト名(FQDN)を使用しています

ホスト名	種別
websrv.contoso.com (Lync 外部公開ホスト名)	サブジェクト名, 別名
dialin.contoso.com (電話会議外部公開ホスト名)	別名
meet.contoso.com (会議用外部公開ホスト名)	別名
lyncdiscover.contoso.com (オートディスカバーホスト名)	別名
wac2.contoso.com(Office Web Apps 公開ホスト名) – オプション(単独で証明書を発行する場合には、必要無)	別名

注意 ： 今回個別で実施する Office Web Apps サーバー外部公開 URL 向けの Web サーバー証明書要求では、サブジェクト名、別名として wac2.contoso.com を指定します。
本書では、Lync フロントエンドプール外部公開 URL 向け Web サーバー証明書の要求手順だけを記載しており、Office Web Apps サーバー外部公開 URL 向け Web サーバー証明書要求は同様の手順で別途実施する必要がありますのでご注意ください。

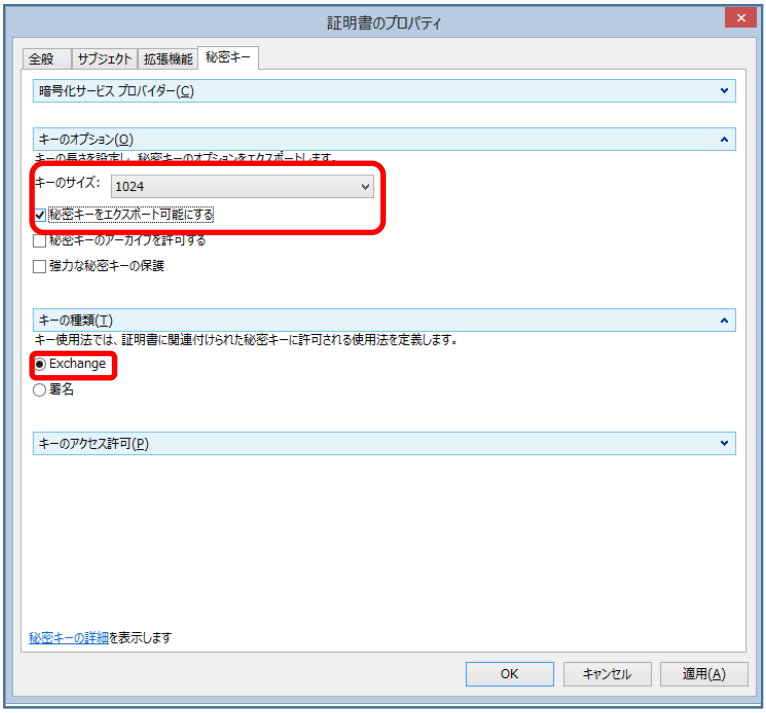


続いて、”拡張機能”タブの”拡張キー使用方法(アプリケーションポリシー)(E)”で”利用可能なオプション:”から”サーバー認証”を選択し追加します。

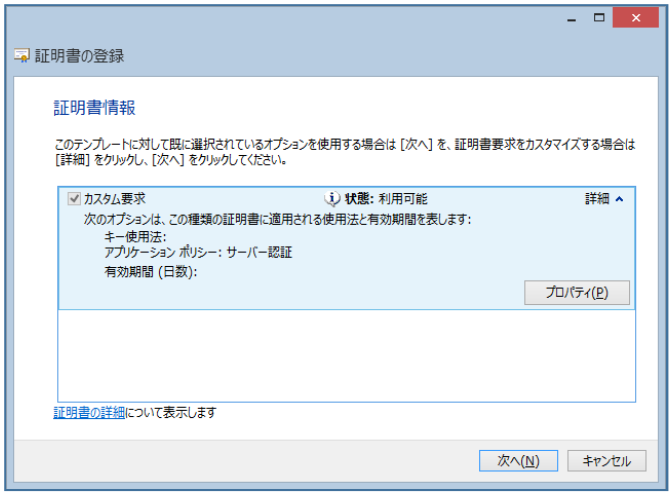


秘密キータブを選択し、”キーの種類(T) “で”Exchange”、”キーのオプション(O) “で”秘密キーをエクスポート可能にする”を選択し、”OK”をクリックします。

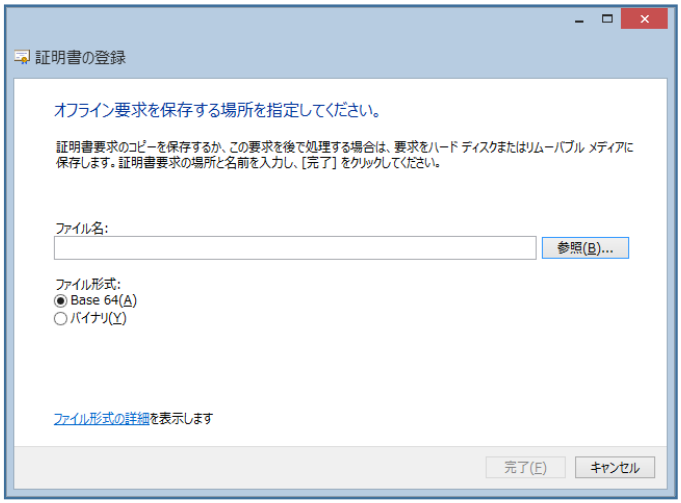
注意 ： キーのサイズを既定のセキュリティポリシーに合わせる必要性がある場合も想定されますので、必要に応じて事前に IT 管理者等に確認して下さい。

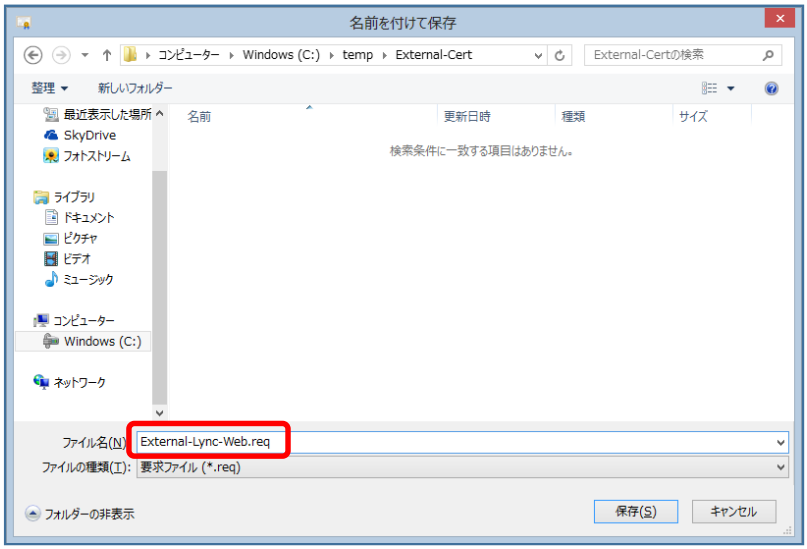


“次へ(N)”をクリックします。

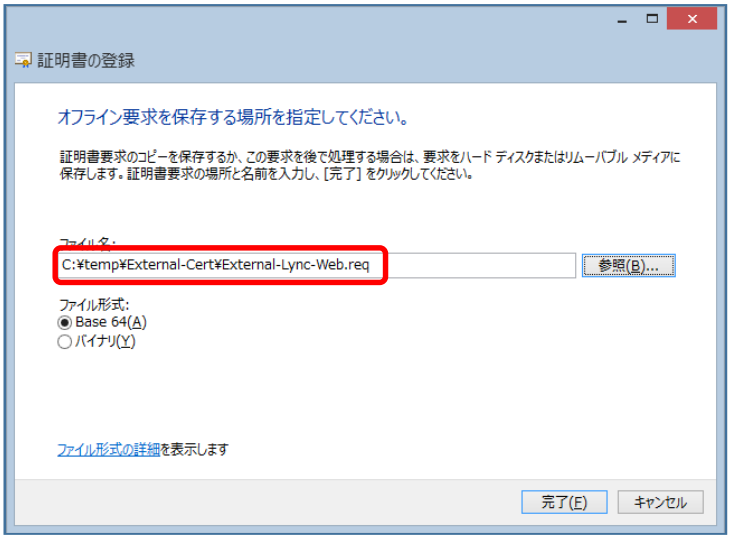


以下の画面で、オンライン要求を保存する場所を指定します。”参照(B)…”をクリックし、保存フォルダー選択並びにファイル名を入力後 保存(S)をクリックします。





ファイル形式で”Base64(A)”を選択後、完了(E)をクリックして終了します。



注意 ：Windows の証明書メニューや IIS を利用して証明書要求ファイルを作成した場合には、秘密鍵の保存を OpenSSL のように証明書発行前に実行することができませんのでご注意ください。

Windows PC 端末で要求ファイルを作成した場合には、要求ファイルを作成した Windows PC 端末に発行された証明書をインポートした後、秘密鍵付きの証明書をエクスポートすることができます。

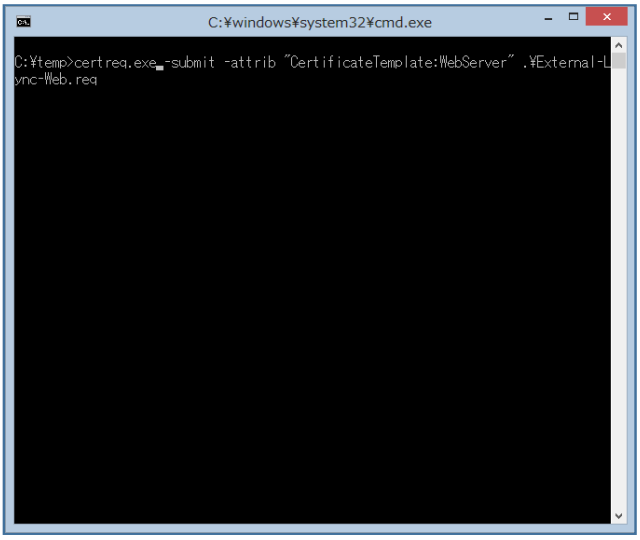
5.2　証明書の発行

注意 ： 本書のシナリオでは、ベリサインやジオトラストの様な公開認証局を利用せず、Windows サーバーの証明機関(CA)を利用しており、実際に公開証明書を取得する方法とは異なりますのでご注意ください。
作成した証明書要求ファイル(CSR)を利用して、公開認証局から証明書を取得する方法に関しては、各公開認証局迄お問い合わせください。

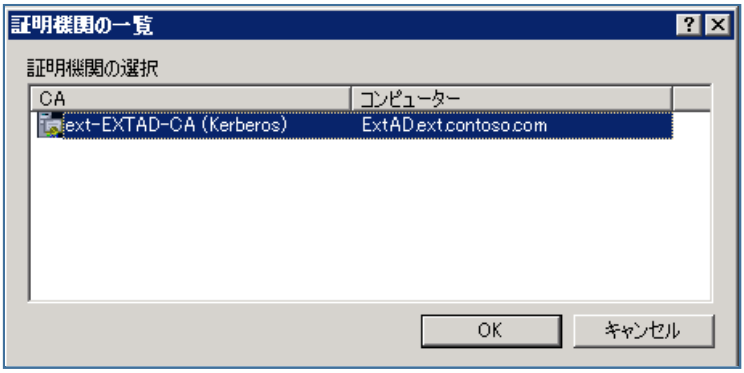
先ほど作成した CSR ファイルを、Windows サーバー(認証局として証明機関が役割で追加されている)がアクセスできるフォルダへコピー等を事前に実施しておきます。

証明書テンプレートで Web サーバーを指定して要求を実行する必要があるため、コマンドプロンプトを開き、以下のコマンドを実行します。

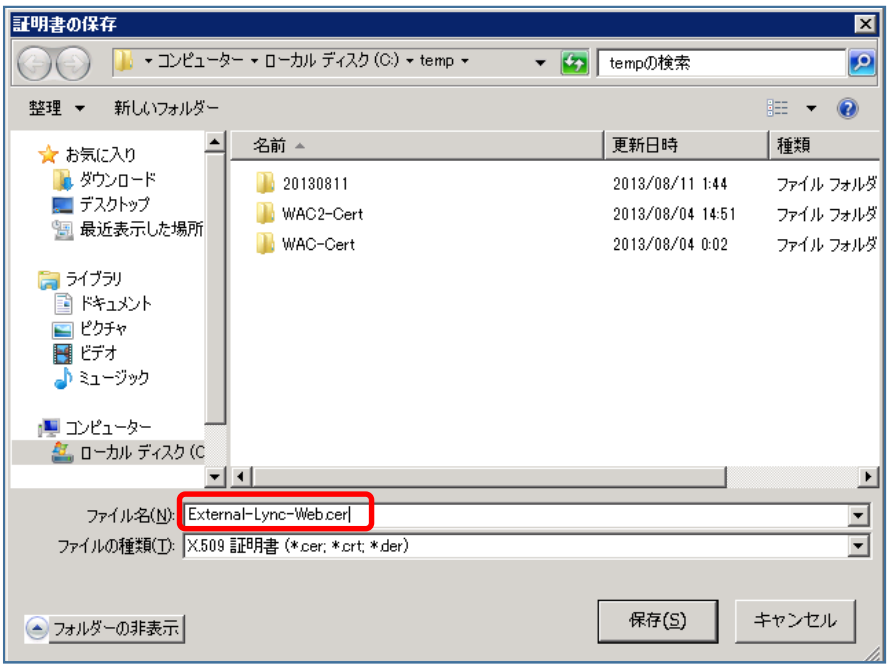
certreq.exe -submit -attrib “CertificateTemplate:WebServer” 要求ファイル名



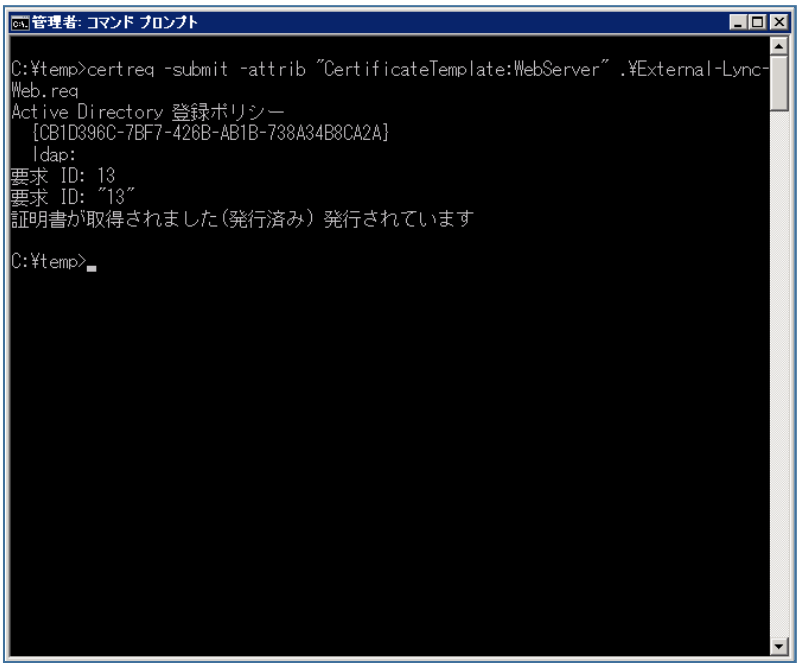
証明機関の一覧で証明機関を確認し、”OK”をクリックします。



証明書の保存画面がポップアップされるので、適切なフォルダ、ファイル名を指定して”保存(S)”を実行します。

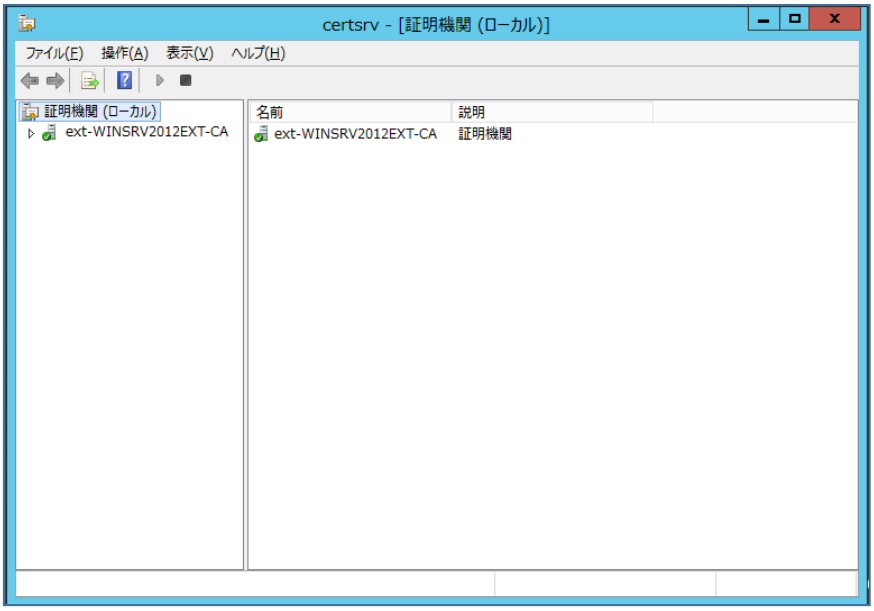


画面上で、証明書が正常に発行されたことを確認して終了します。

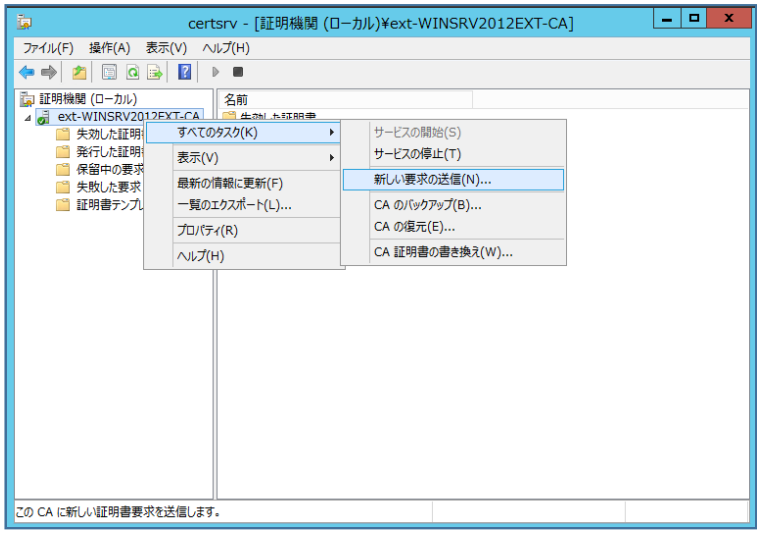


先のコマンドラインの証明書要求を、以下の手順のように証明機関の GUI メニューから実施した場合には、エラーが発生してしまいます。これは、サーバーの証明書要求ファイル作成時にテンプレートを指定しなかったためです。もし、要求ファイルの作成時に Web サーバーのテンプレートを指定することができる環境であれば、先のコマンドラインの代わりに、下記に示す GUI メニューで必要な証明書を発行することができます。

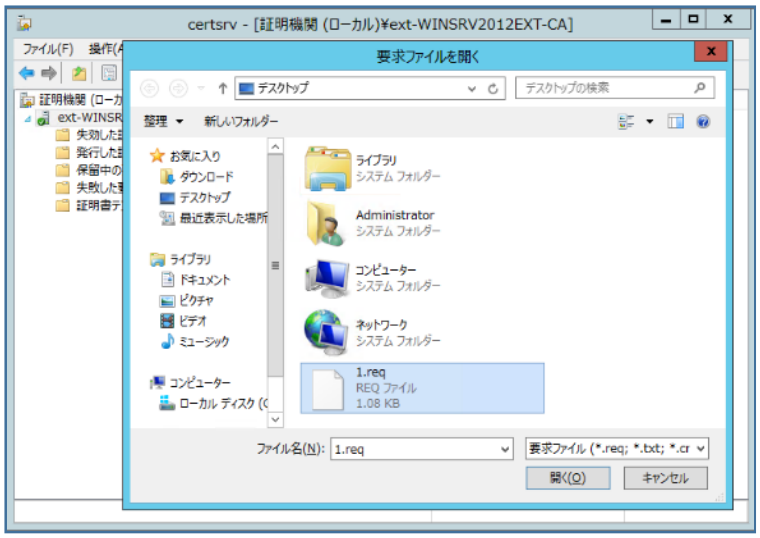
Windows サーバーの”証明機関”をメニューから起動します。



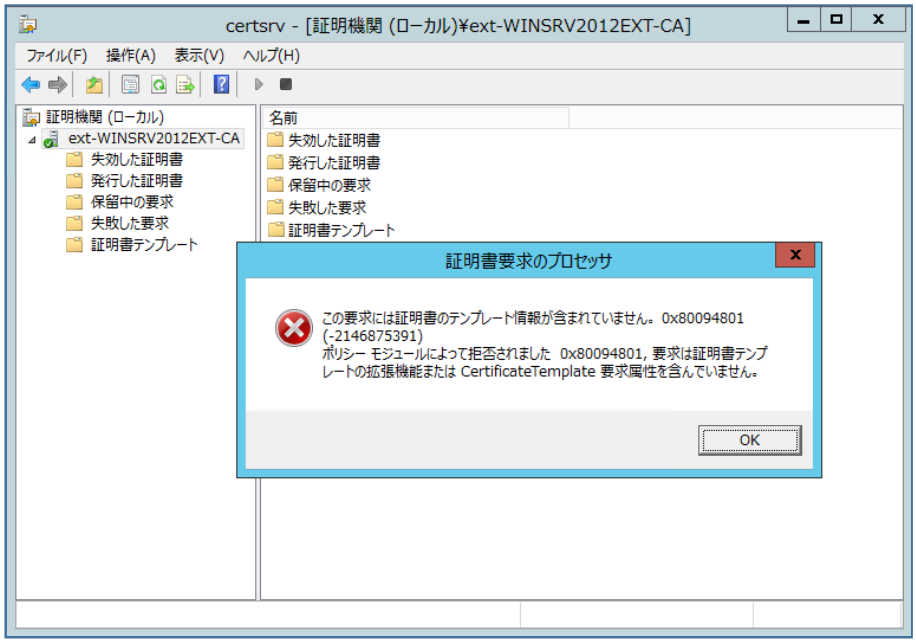
認証局(CA)を右クリックし、”すべてのタスク(K)” >> “新しい要求の送信(N)”を選択します。



保存した要求ファイルを選択し、”開く(O)”をクリックします。



作成した要求ファイルに、証明書テンプレート情報が含まれていない場合、下記のようなエラーメッセージが出力されます。証明書テンプレートとして Web サーバーを選択し要求ファイル（CSR）を作成した場合には、問題なく証明書は発行されます。

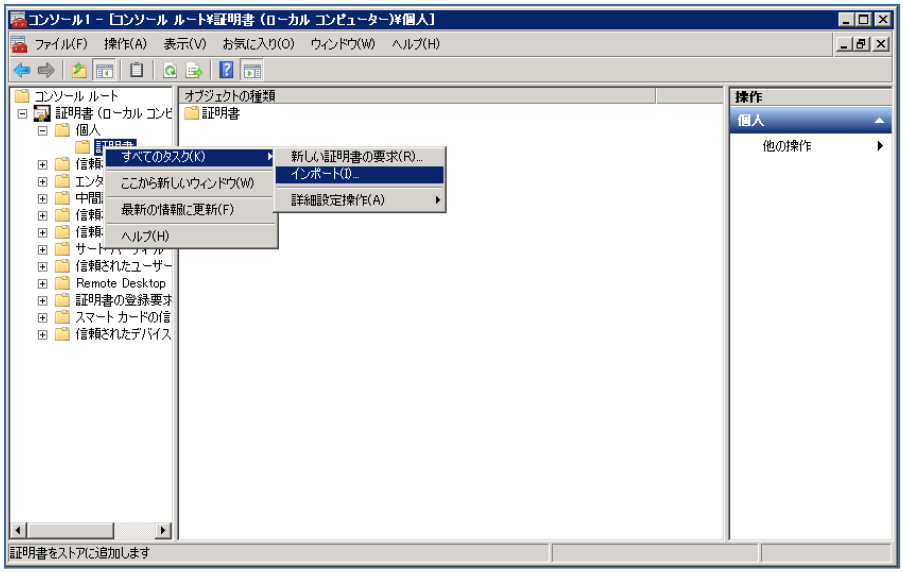


5.3　証明書要求 PC への証明書のインポートと秘密鍵付き証明書のエクスポート

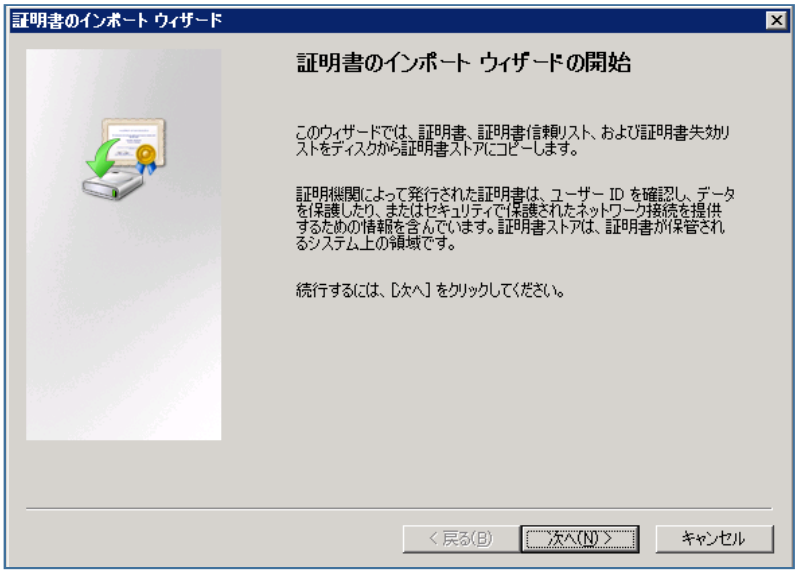
5.3.1 証明書インポート

先ほど発行した Web サーバー証明書を、証明書を要求した PC が読み取れるフォルダーへコピー等を実行します。

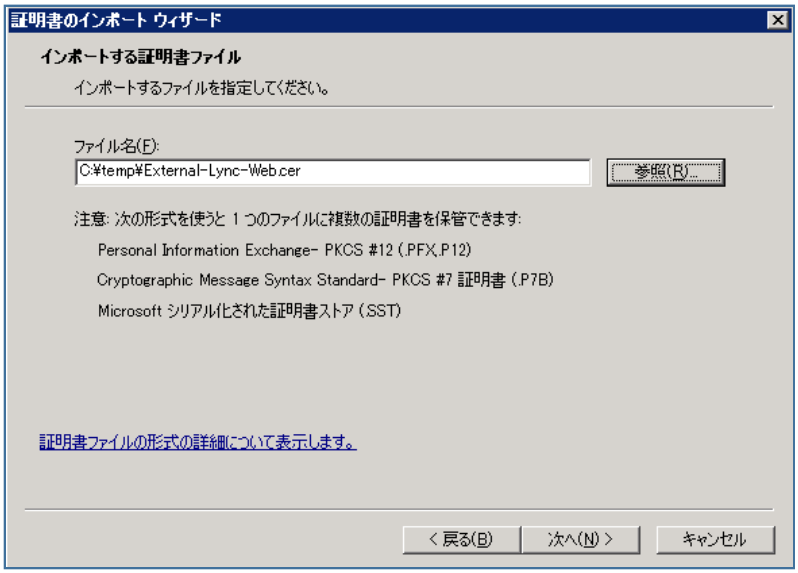
証明書を要求した Windows PC 端末で、再度 mmc のスナップインで証明書を立ち上げ、”証明書(ローカルコンピューター)” >> “個人”を選択し右クリックで”インポート(I)”を実行します。



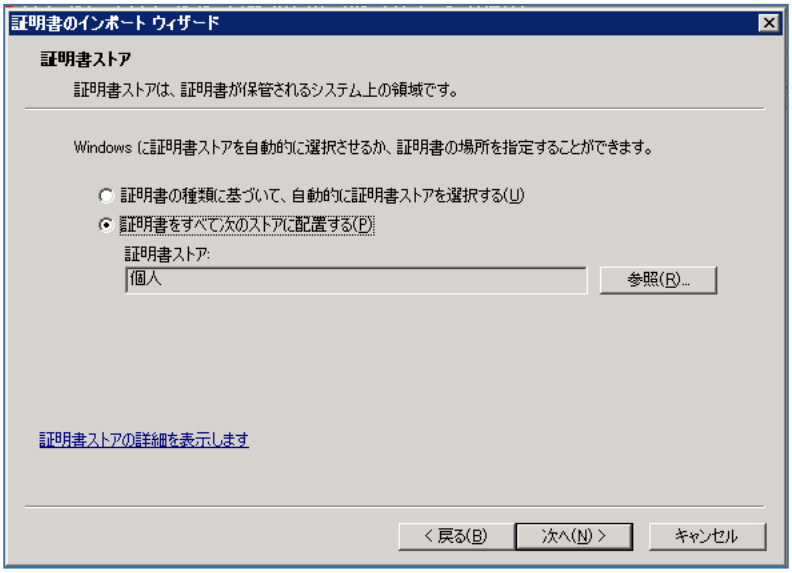
証明書インポートウィザードが開始されますので、”次へ(N)”をクリックします。



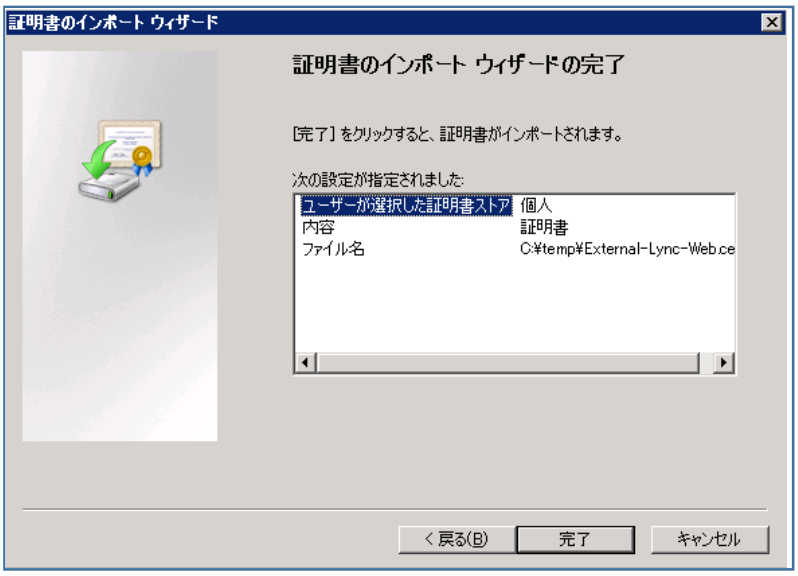
先ほど発行した証明書ファイルを選択し、”次へ(N)”をクリックします。

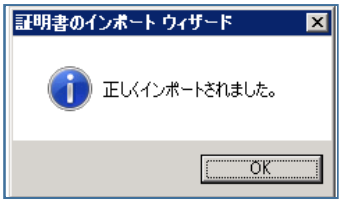


証明書ストアで”個人”が選択されていることを確認(個人でない場合には、個人を選択し直します)し、”次へ(N)”をクリックします。

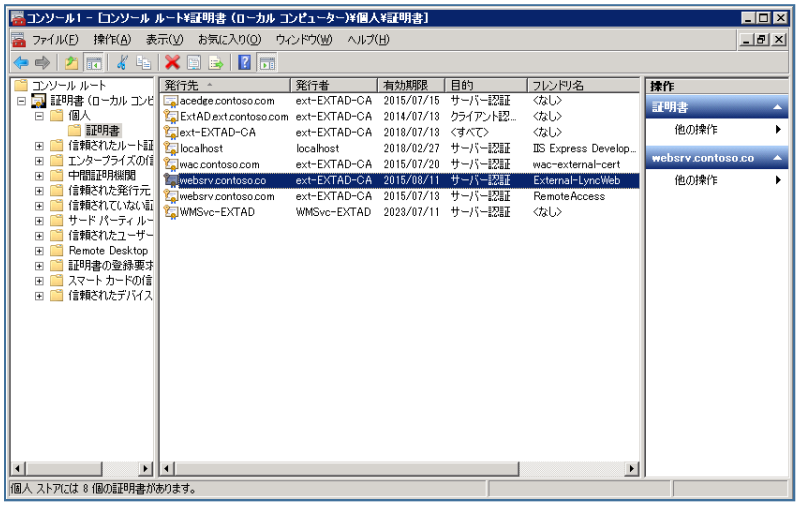


最終的な確認画面が表示されるので、証明書ストアが”個人”で、選択されているファイルが正しいことを確認し、”完了”をクリックして Web サーバー証明書のインポートを完了します。





“個人” >> “証明書”をクリックし、個人ストアに、先ほどインポートした証明書が正しく反映されていることを確認します。

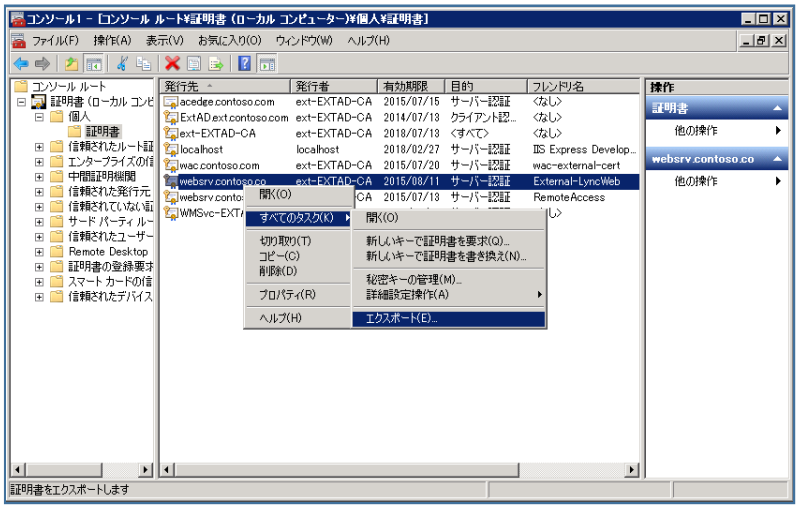


注意 ： インポートの失敗もしくは、インポートしても個人ストアにうまく反映されない場合の要因として、証明書を発行した認証局(CA)のルート証明書が、当該 PC の信頼されたルート証明機関に存在しないことが考えられます。このような場合には Web サーバー証明書を発行した認証局のルート証明書をエクスポートし、当該 PC に信頼されるルート証明書としてインポートする必要があります。

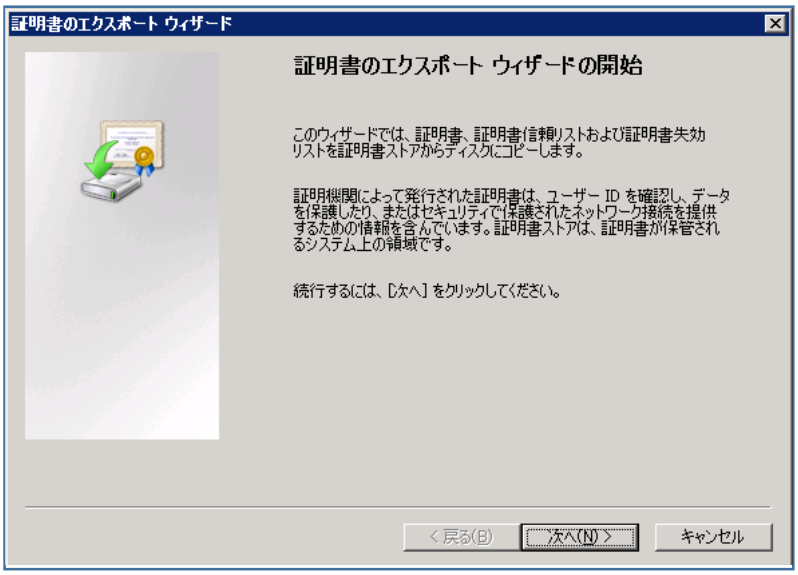
5.3.2 証明書エクスポート

先ほどインポートした証明書を SoftAX で利用するため、秘密鍵付きの pfx 形式でエクスポートします。

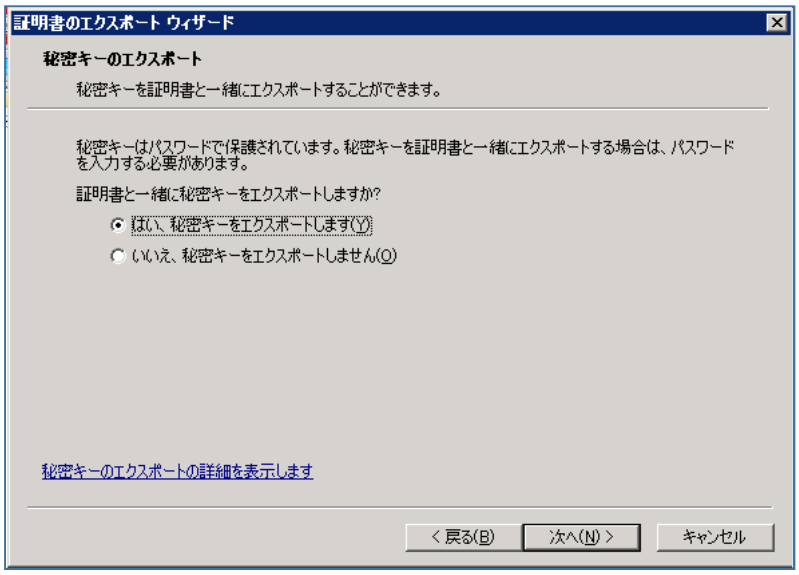
証明書画面で、先ほど個人ストアにインポートした証明書を選択し、”右クリック” >> “すべてのタスク(K)” >> “エクスポート(E)”を選択します。



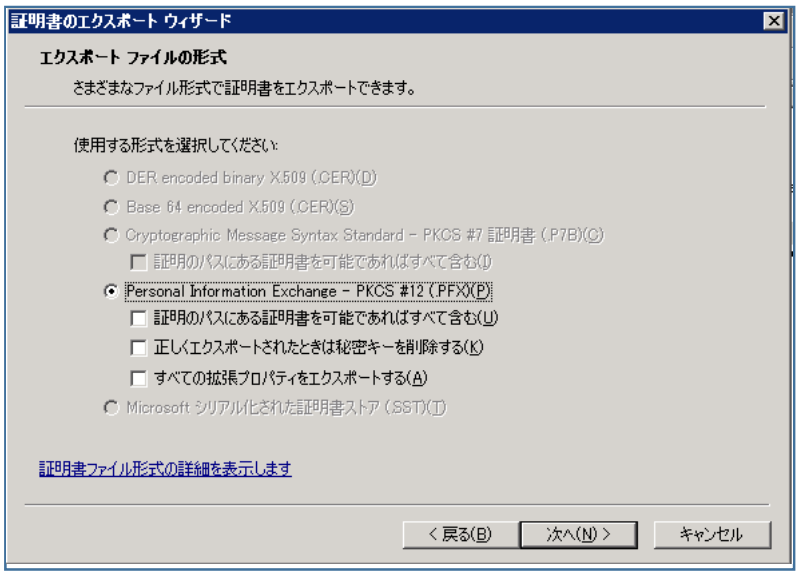
証明書エクスポートウィザードが展開されるので、”次へ(N)”をクリックします。



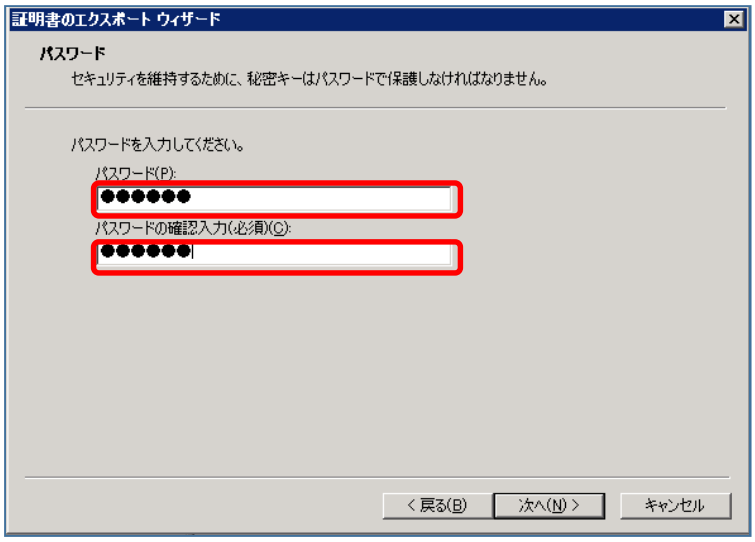
“証明書と一緒に秘密キーをエクスポートしますか?”で、”はい、秘密キーをエクスポートします(Y)”をチェックし、”次へ(N)”をクリックします。



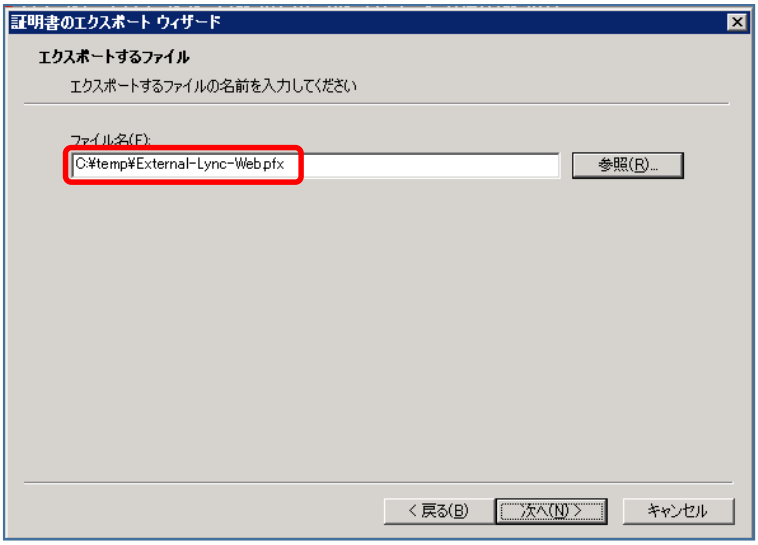
エクスポート ファイル形式として”Personal Information Exchange – PKCS #12 (.PFX)(P)”をチェックし、”次へ(N)”をクリックします。



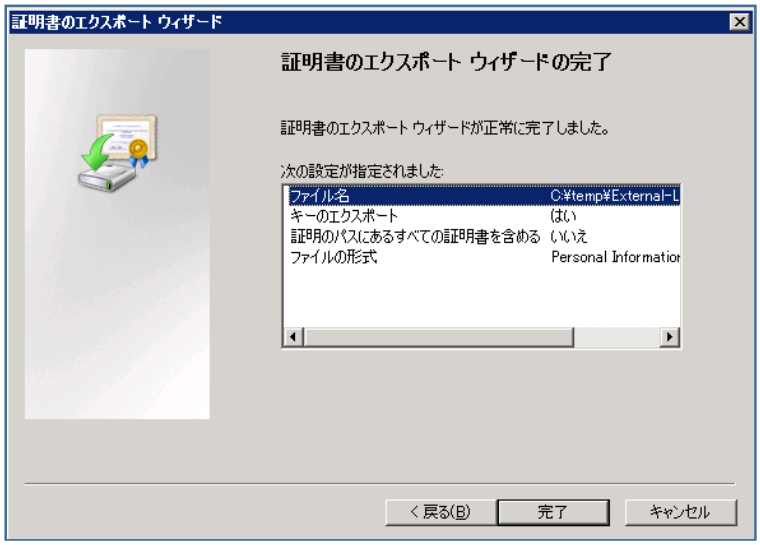
秘密鍵を保護するための”パスワードを入力(後の SoftAX での証明書インポート時に使用します)後、”次へ(N)”をクリックします。

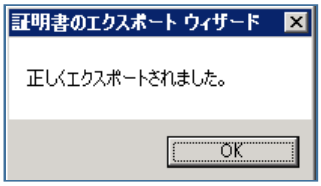


エクスポートするファイル名で、保存するフォルダ、ファイル名を指定して”次へ(N)”をクリックします。



エクスポートの条件やファイル名等を再確認した上で、”完了”をクリックし、証明書ファイルの秘密鍵付きエクスポートを完了します。

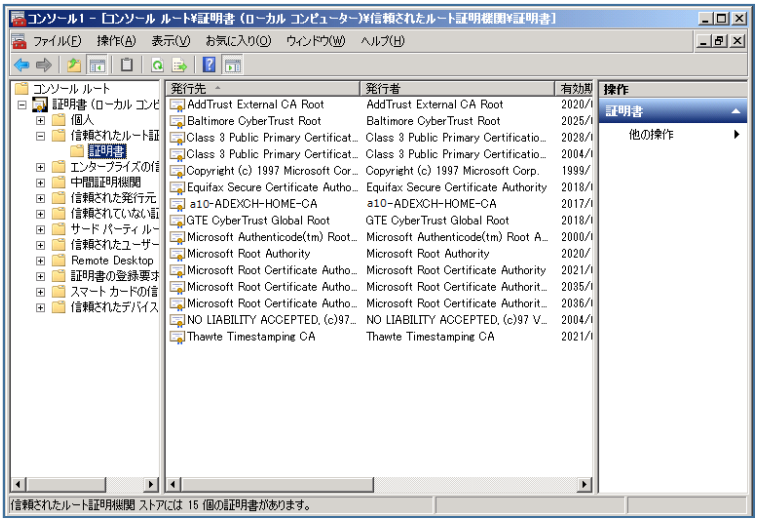


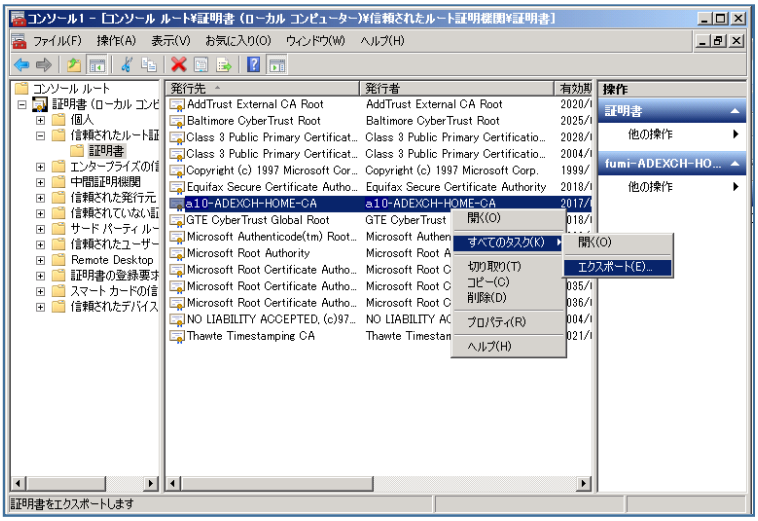


5.4 内部認証局(CA)のルート証明書エクスポート

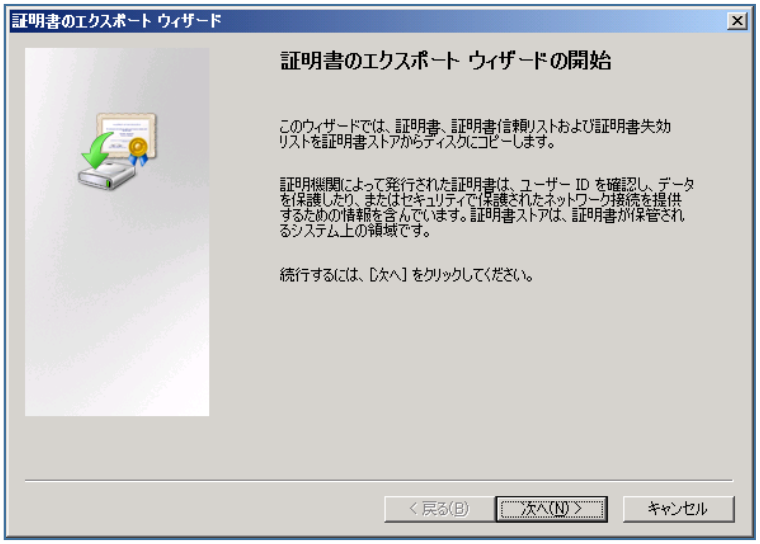
SoftAXが内部(社内)ネットワークに展開されているLyncフロントエンドサーバーやOffice Web Apps サーバーと SSL セッションを開設するにあたり、それらのサーバーが利用している Web サーバー証明書を発行した内部認証局(CA)のルート証明書を、信頼されたルート証明機関としてインポートする必要があります。
ここでは、SoftAX へインポートする内部認証局(CA)のルート証明書をエクスポートする手順を記します。

内部認証局(CA)のルート証明書を保持している Lync フロントエンドサーバーや Office Web Apps C サーバー上で、mmc のスナップイン経由で証明書を立ち上げ、”信頼されたルート証明機関”を開き、内部認証局(CA)のルート証明書を選択し、”右クリック” >> “すべてのタスク(K)” >> “エクスポート(E)”で、エクスポート処理を開始します。

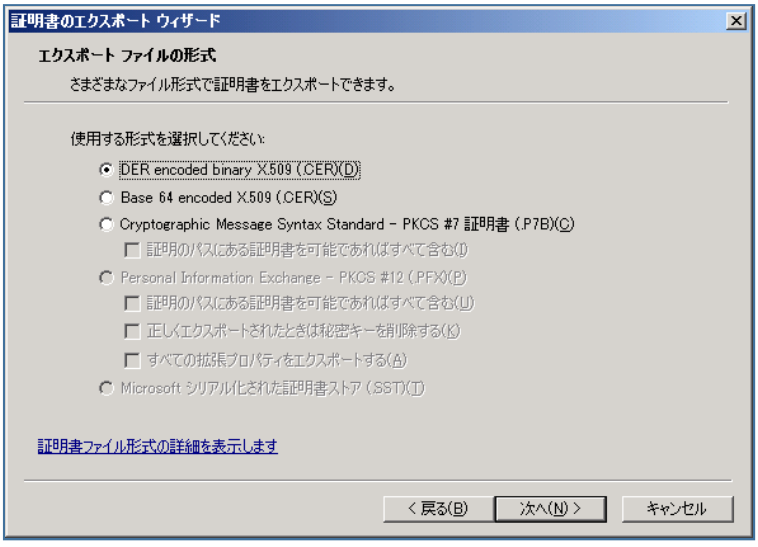




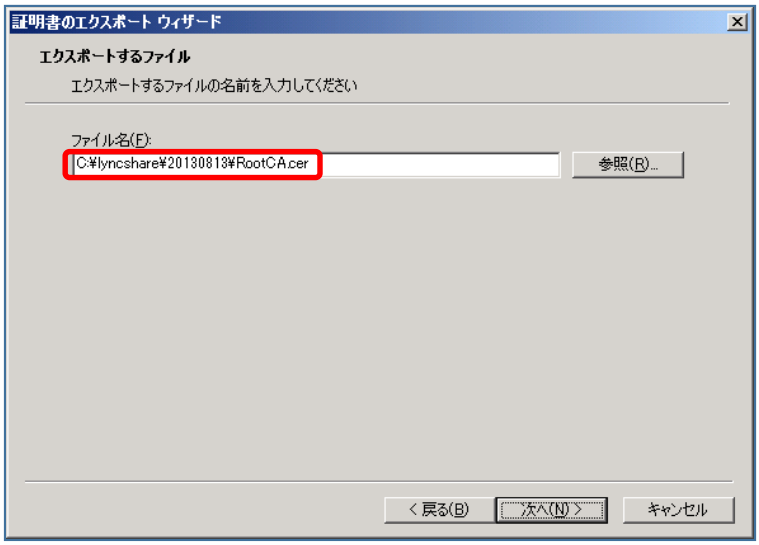
エクスポートウィーザードが開始されるので、”次へ(N)”をクリックします。



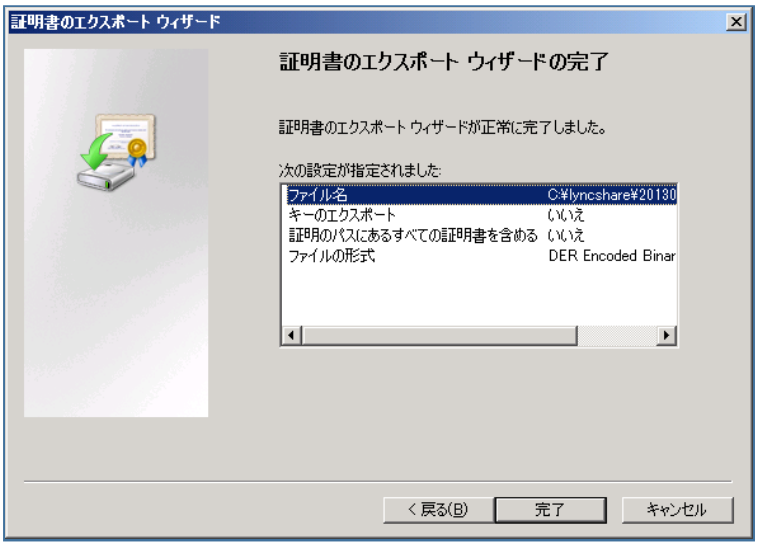
エクスポート ファイル形式で、適当な形式を選択(今回はデフォルトの”DER encoded binary X.509 (.CER)(D)”を選択)し、”次へ(N)”をクリックします。

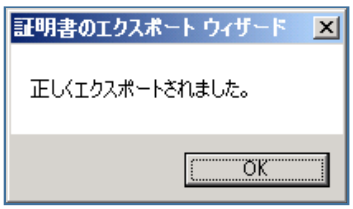


エクスポートするルート証明書を保存するフォルダ、ファイル名を指定し、”次へ(N)”をクリックします。



エクスポートする証明書のファイル名、ファイル形式を確認し、”完了”をクリックし終了します。





6 SoftAX の構成

以下は、SoftAX の動作要件です。

6.1 SoftAX の要件

6.1.1 ハードウェア要件

CPU : 1 (Intel-VT-enabled もしくは AMD-V)

メモリ : 最低 2GB

ディスク容量 : 20GB

ネットワークアダプター : 2 つ以上のイーサーネットアダプター (3 つ以上を推奨)

6.1.2 仮想マシン要件

仮想 CPU : 1

メモリ : 最低 2GB

ディスク容量 : 8GB

ネットワークアダプター : 3 つ以上の仮想ネットワークアダプターを推奨

管理用 x 1, データ用 x 2

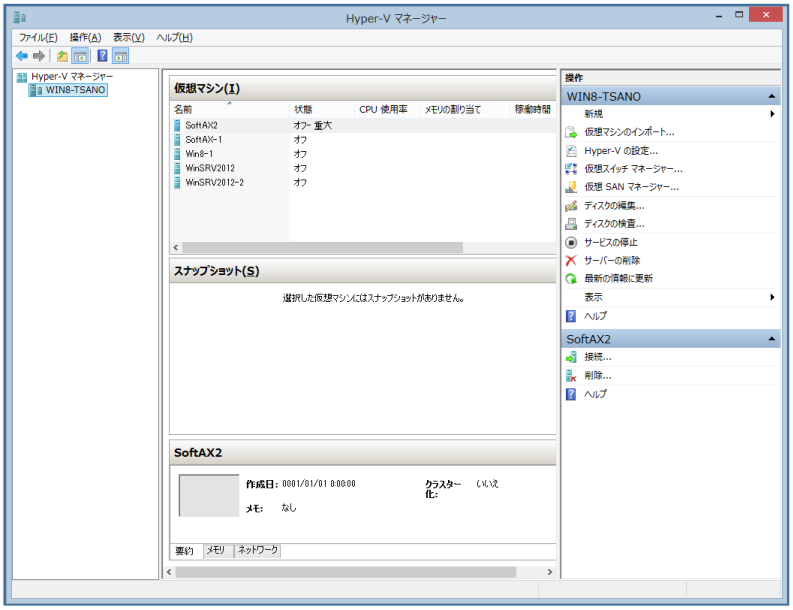
注意 : 本書の検証では、SoftAX のプラットフォームとして Windows Server 2008R2 上の Hyper-V を利用しています。SoftAX はこの他に、VMWare vSphere、KVM、Citrix Xen、Amazon EC2 の仮想化ソリューションもサポートしています。

6.2 Hyper-V の準備

Hyper-V 上で SoftAX を利用するにあたり、まず必要な仮想ネットワークを作成します。

今回は管理用 x1、データ用 x2 の仮想ネットワークを定義します。

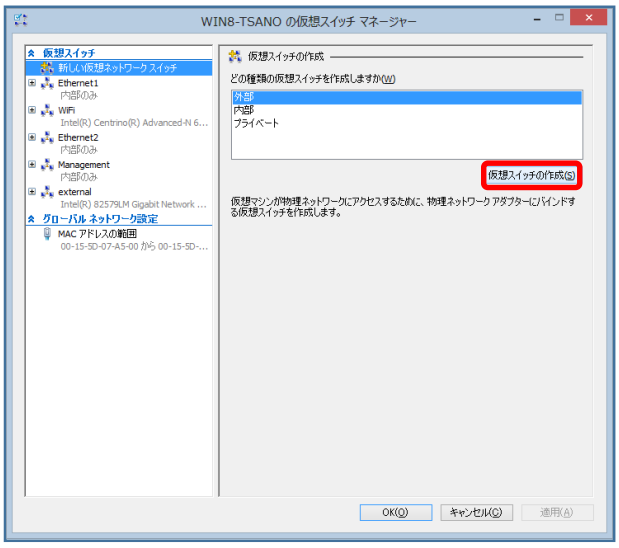
Hyper-V マネージャーを立ち上げ、右パネの”仮想スイッチマネージャー…”を選択します。



本書のシナリオでは、仮想スイッチマネージャーで以下の仮想スイッチを定義します。

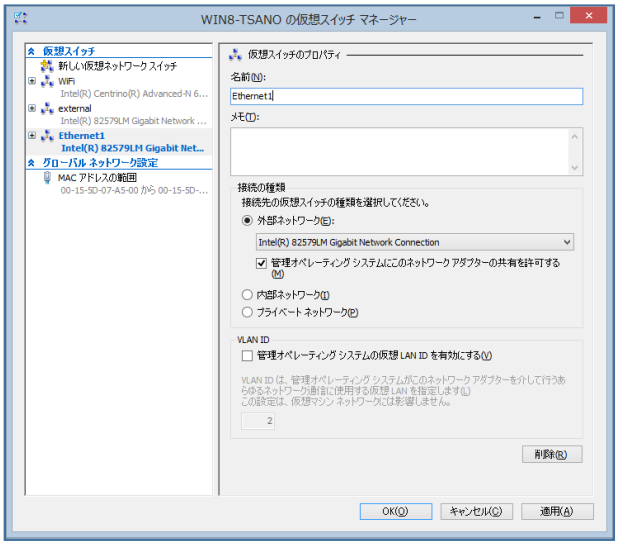
- Management　(SoftAX 管理用)
- Ethernet1 (外部ネットワーク向け)
- Ethernet2 (内部ネットワーク向け)

“仮想スイッチの作成(S)”をクリックし、上記の 3 つのインターフェースを各々設定していきます。



下記に Ethernet1 の設定例を示します。”名前(N):”に”Ethernet1”、”接続の種類”から適切な仮想スイッチ(本書のケースでは、Ethernet1 を外部公開用ネットワークインターフェースとしています。)を選択し、割り当てていきます。

同様の手順で、Management、Ethernet2 を定義し、各々に適切なネットワークインターフェースを割り当てていきます。



以上で、Hyper-V の初期設定は完了となります。

続いて、Hyper-V 向け SoftAX の展開を実施していきます。

6.3 SoftAX の展開 (Hyper-V 編)

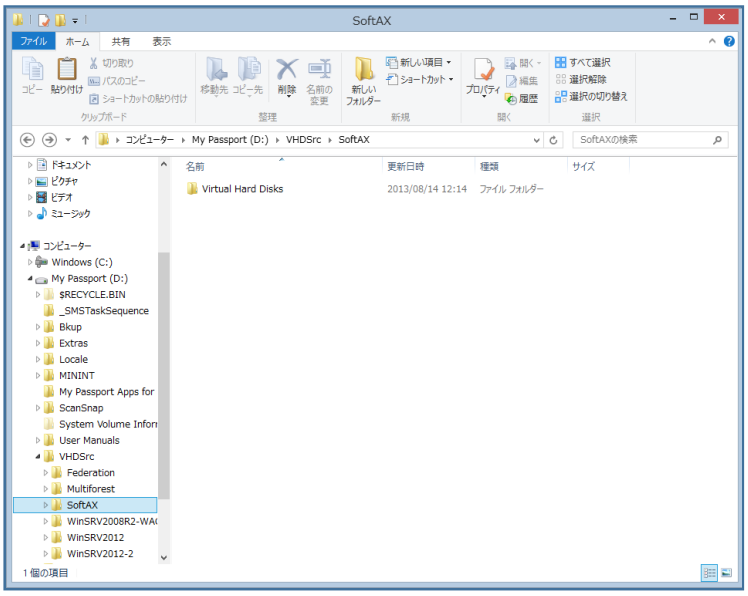
入手した SoftAX のインスタンスを展開していきます。

注意 ：SoftAX のライセンスは、仮想インスタンス展開後でないと、要求・発行することができませんのでご注意ください。

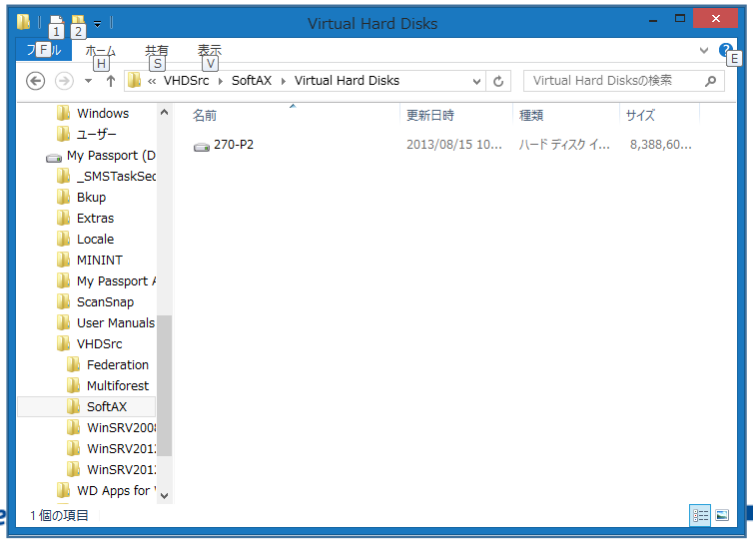
メモ ：

SoftAX の検証用インスタンスと無償ライセンス(30 日有効)は下記 URL からお申し込みいただけますので、商用環境導入前の事前検証等でご利用ください。
http://www.a10networks.co.jp/products/virtualaxseries/softax-trial.html

最初に SoftAX を展開するフォルダを作成します。ここでは親フォルダとして SoftAX、SoftAX インスタンスの保存先として Virtual Hard Disks を作成します。

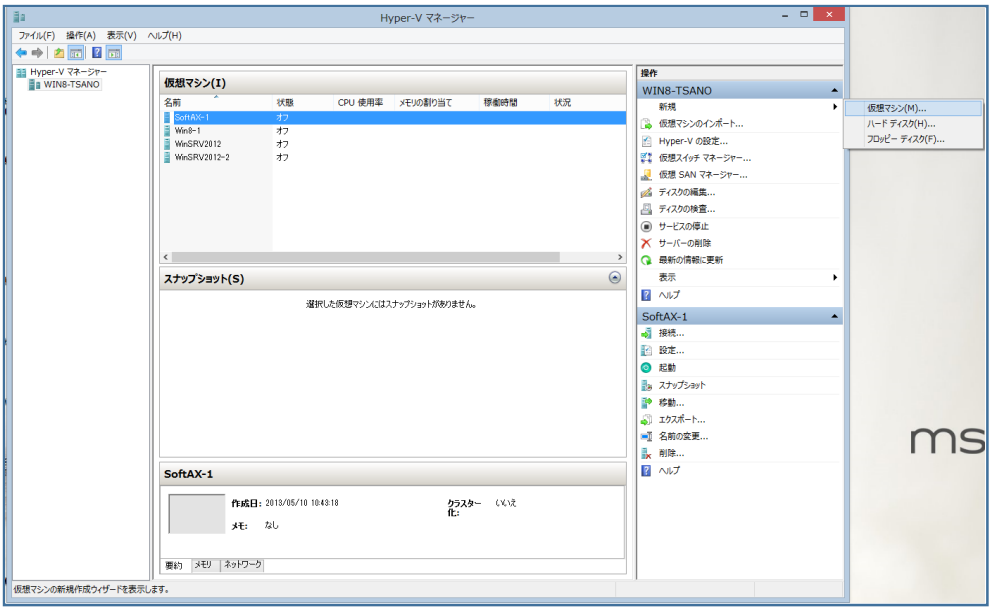


入手した、SoftAX のインスタンスファイルを先ほど作成した保存先フォルダに保存します。

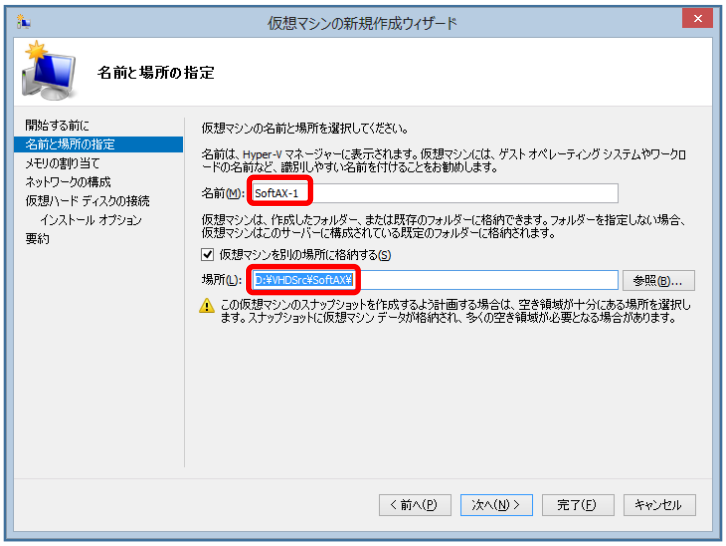


以上で事前準備は完了です。続いて SoftAX のインスタンスを展開します。

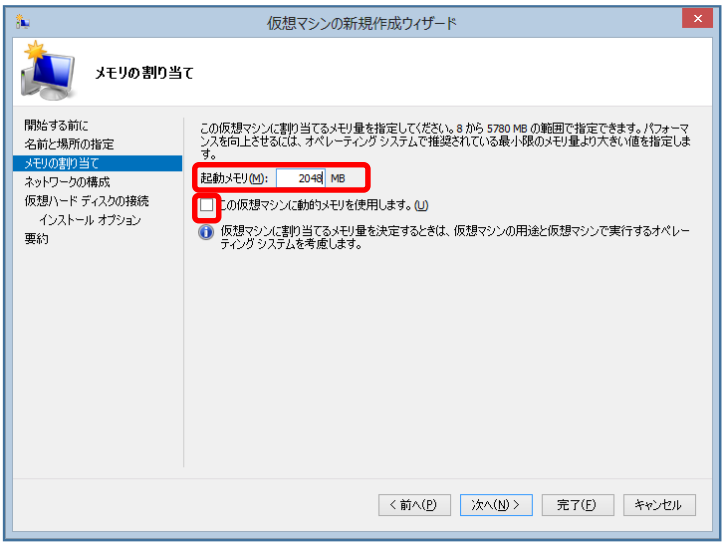
Hyper-V マネージャーの右パネで、”新規” >> “仮想マシン(M)”を選択します。



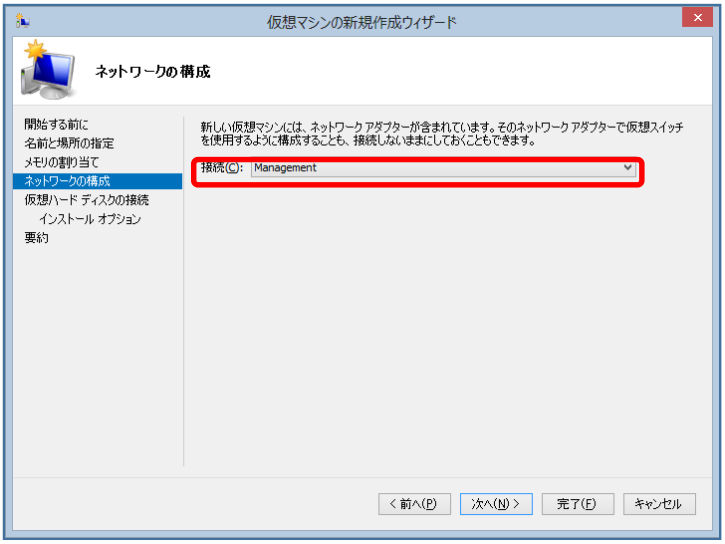
仮想マシンの新規作成ウィザードが現れるので、SoftAX の仮想マシンの名前と仮想マシンを保存する場所を、”名前(M)：”、”場所(L):”に各々設定し”次へ(N)”をクリックします。ここでは、仮想マシン名として SoftAX-1、保存先として、先ほど作成した SoftAX を指定します。



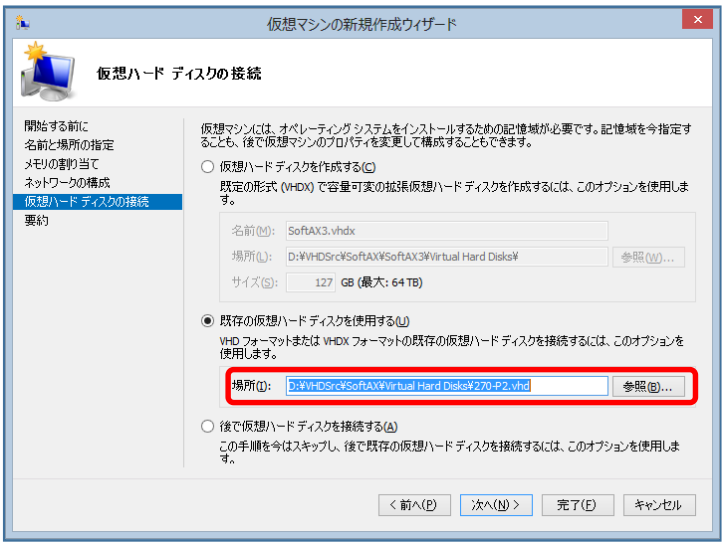
起動メモリとして 2,048 を入力し、”この仮想マシンに動的メモリを使用します。(U)”がチェックされていないことを確認し、”次へ(N)”をクリック



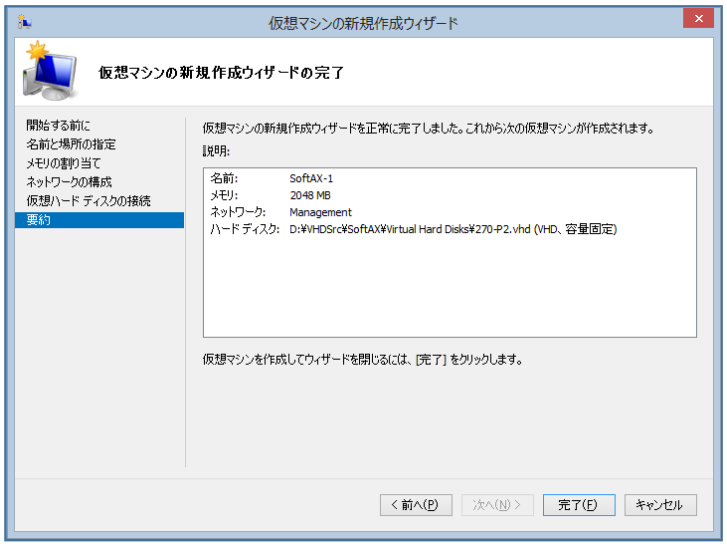
ネットワークの構成で、”接続(C):”に先ほど作成した仮想スイッチの Management を選択し、”次へ(N)”をクリックします。



仮想ハードディスクの接続画面で、”既存の仮想ハードディスクを使用する(U)”を選択し、”場所(I)”として先ほど保存した SoftAX のインスタンスファイルを指定して、”次へ(N)”をクリックします。

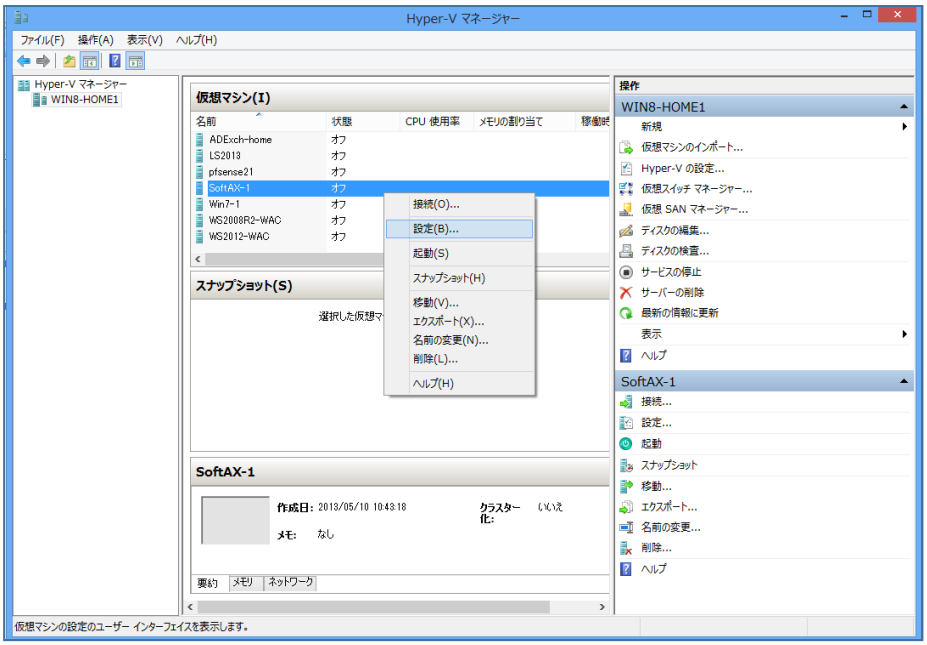


最後に、設定した内容を確認し”完了(F)”をクリックし SoftAX の展開を完了します。

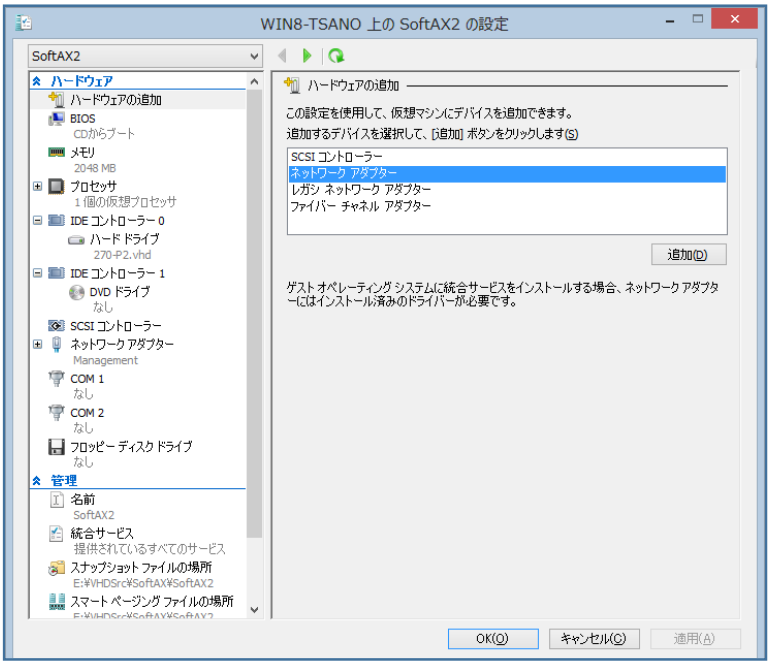


続いて、SoftAX にデータネットワーク向けの仮想スイッチを追加していきます。

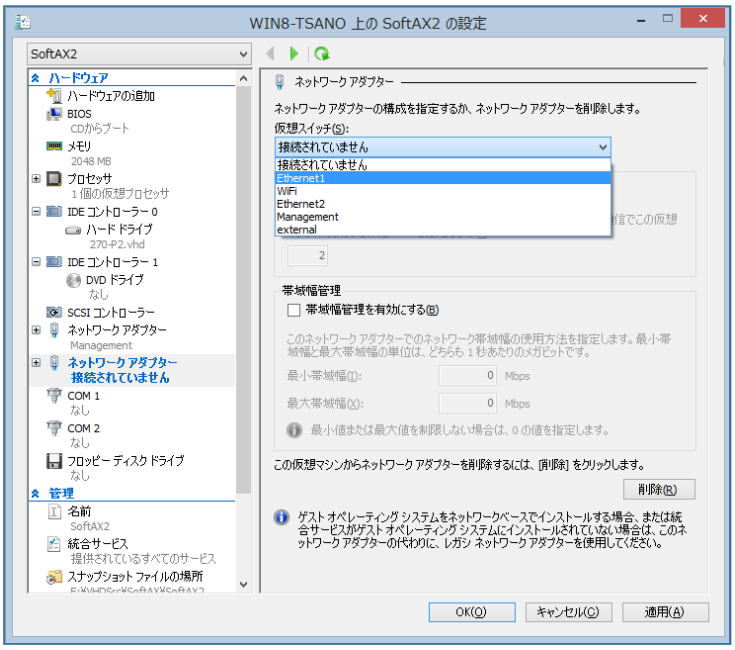
Hyper-V マネージャーで作成した SooftAX の仮想マシンを選択し、右クリックで”設定(B)…”を開きます。

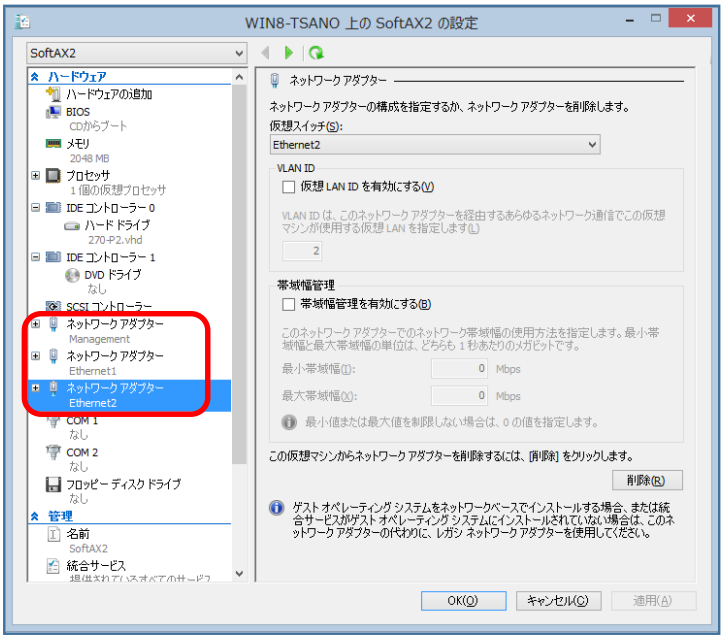


左パネの”ハードウェアの追加”を選択し、追加するデバイスで”ネットワークアダプター”を選択して”追加(D)”をクリックします。



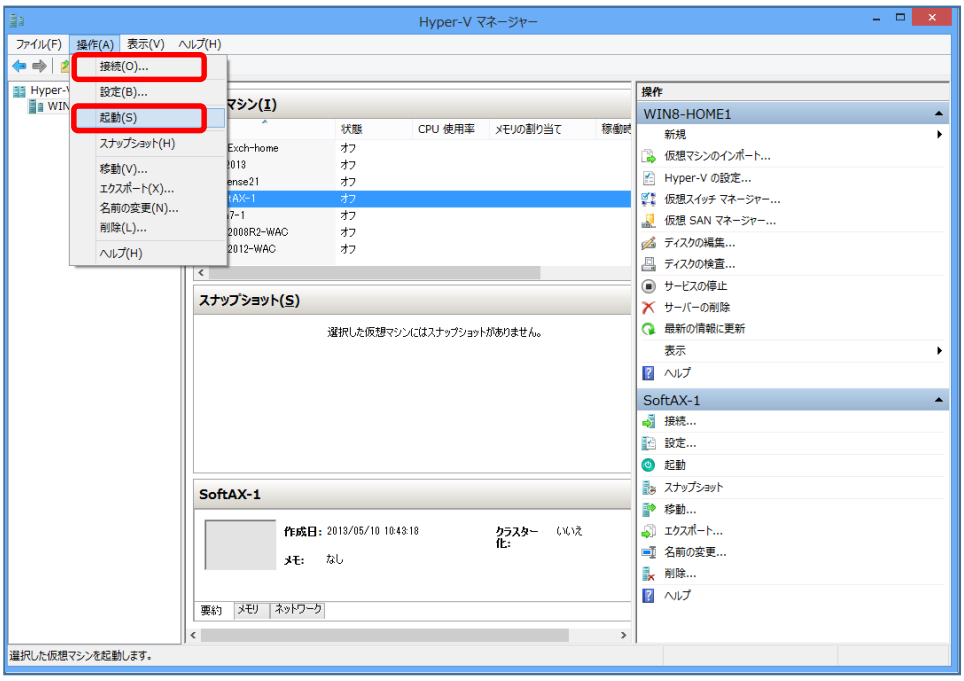
“仮想スイッチ(S):”として、先ほど定義した Ethernet1 と Ethernet2 を追加し、”OK(O)”をクリックして終了します。

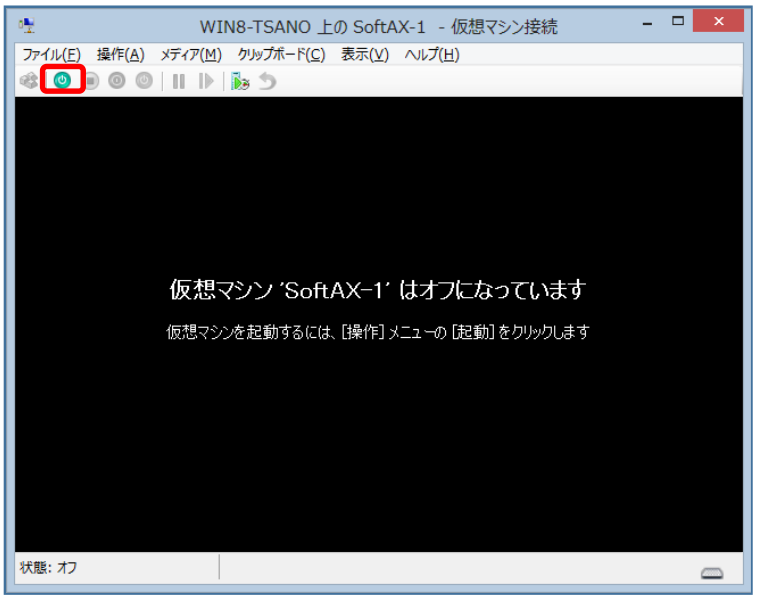


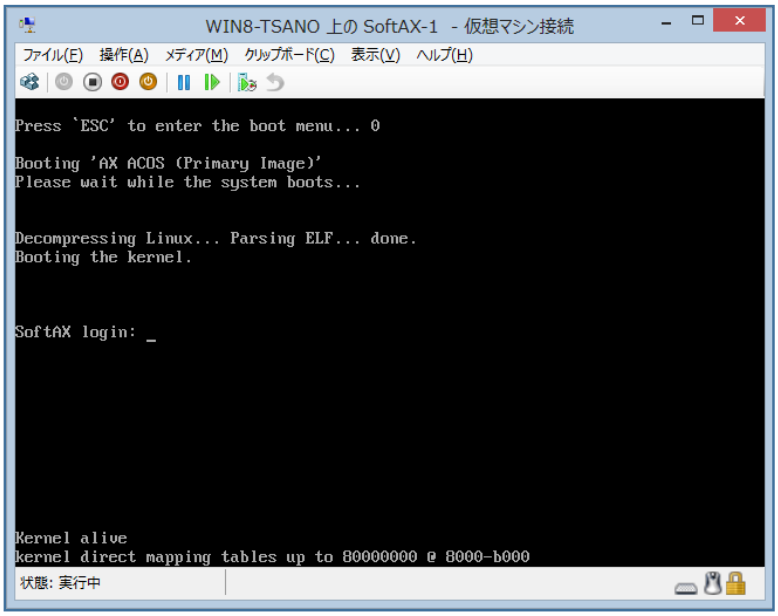


6.4 SoftAX 初期設定

SoftAX の仮想マシンに接続し、”起動(S)…”、もしくは起動ボタンをクリックして SoftAX を起動します。

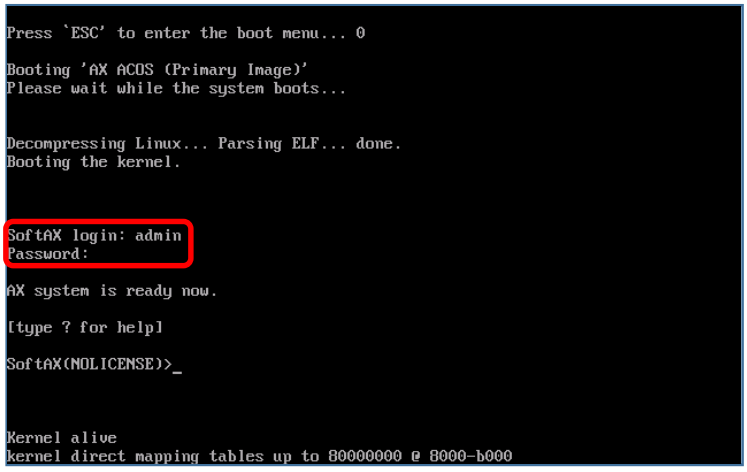




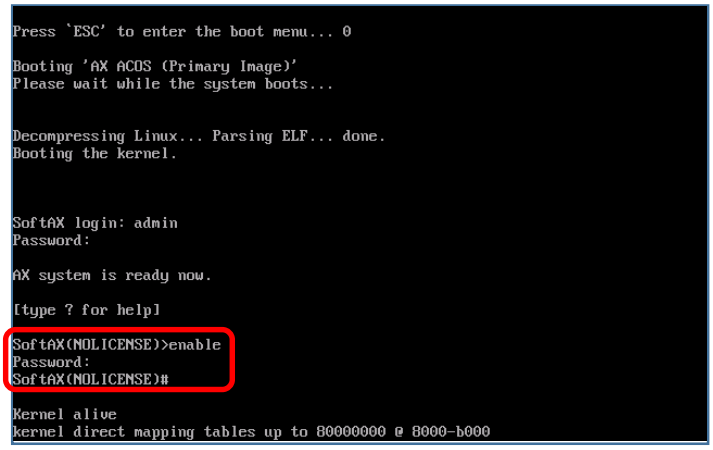


ログイン画面で、デフォルトのユーザー名 : “admin“、パスワード : “a10“を入力し、ログインします。

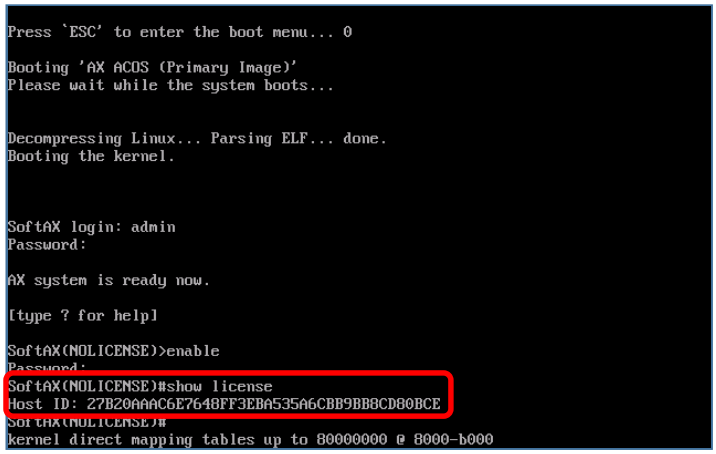
注意 : この時点で SoftAX にはまだライセンスが適用されていないため、NOLICENSE モードで立ち上がります。
NOLICENSE モードでは、データパケットは処理されませんので、負荷分散装置として動作させることはできません。



コマンドライン上で、”enable”と入力し、”Password”には何も入力しないで Enter キーを押して、Enable モードに遷移します。



ライセンスを発行するための、ホスト ID を”show license”で表示させます。



上記で入手したホスト ID を書き記し、所定のライセンス発行手続きを経て正式版ライセンスを入手します。無償評価ライセンス(30 日)の入手方法は、6.3 章を参照してください。

注意：Hyper-V マネージャーの仮想マシン接続画面では、コマンドライン上に表示されたホスト ID をテキストとしてコピーすることはできません。もしホスト ID をコピーしたい場合には、管理インターフェース(仮想スイッチ：Management)経由で、SSH クライアント、もしくはブラウザ経由でログインする必要があります。

管理インターフェースのデフォルト IP アドレスは、172.31.31.31/24 となります。管理インターフェースに設定されている IP アドレスに接続するためには、アクセスする PC から IP 接続可能なことが条件となりますので、必要に応じてネットワークルートの追加や、管理用インターフェースに割り当てられている IP アドレスの変更を実施してください。

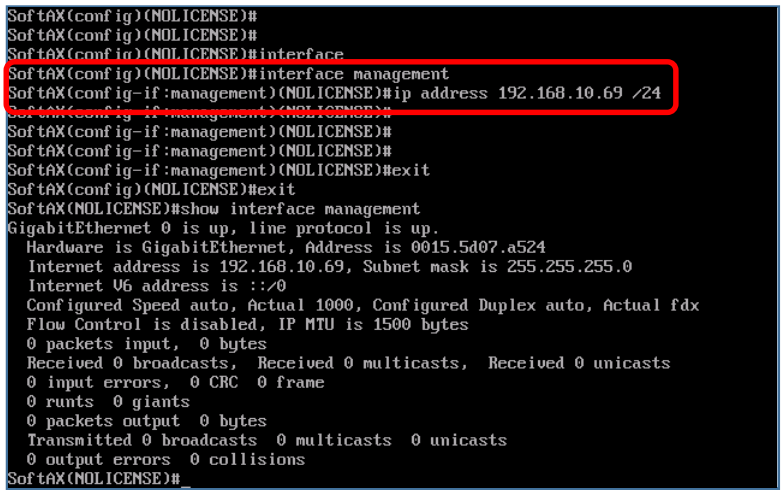
入手したライセンスを SoftAX に適用します。

ここでは、Webベースの GUI メニューからライセンスを適用する方法を記しています。

本書の環境では、設定用 PC と SoftAX を接続するため、管理インターフェースの IP アドレスを以下の方法で変更しています。

configure と入力し、設定モードにした上で、以下の様に管理用 IP アドレスを変更します。

SoftAX(NOLICENSE) # configure
SoftAX(configure)(NOLICENSE) # interface management
SoftAX(configure-if:management)(NOLICENSE) # ip address 192.168.10.69 /24(サブネットマスク)
SoftAX(configure-if:management)(NOLICENSE) # exit
SoftAX(configure)(NOLICENSE) #show interface management (設定確認用)

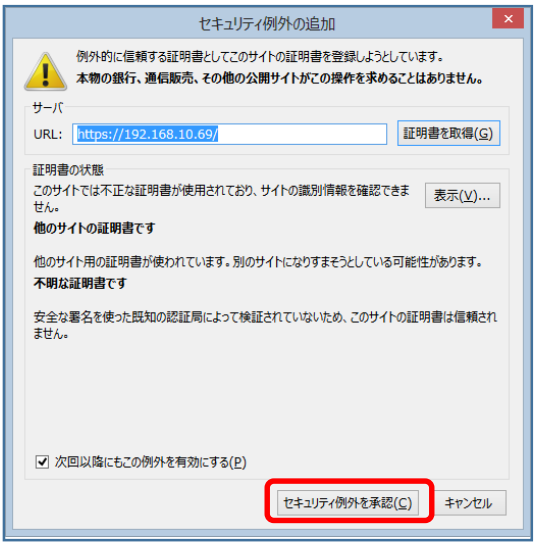


変更した管理用 IP アドレスへ接続するため、SoftAX にデフォルトゲートウェイを設定する必要がある場合には、以下のような設定を実行します。

SoftAX(configure-if:management)(NOLICENSE) # ip default-gateway “ゲートウェイの IP アドレス”

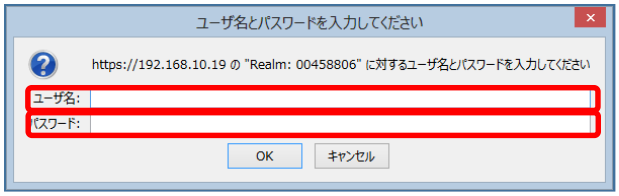
管理インターフェースとの接続設定が終了したら、ブラウザ(今回は FireFox を利用)を開き、https://管理用インターフェースの IP アドレス/と入力します。

SoftAX が利用している Web サーバー証明書を発行した認証局(SoftAX 内部の認証局)のルート証明書が、アクセスしている PC 上の信頼されたルート証明機関に存在しないため上記のようなエラーがでます。しかし、接続先は SoftAX と分かっているため、ここでは”危険性を理解した上で接続するには”を展開し”例外を追加”を選択した後、”セキュリティ例外を承認(C)”をクリックして SoftAX へのアクセスサイトをセキュリティの例外として追加します。



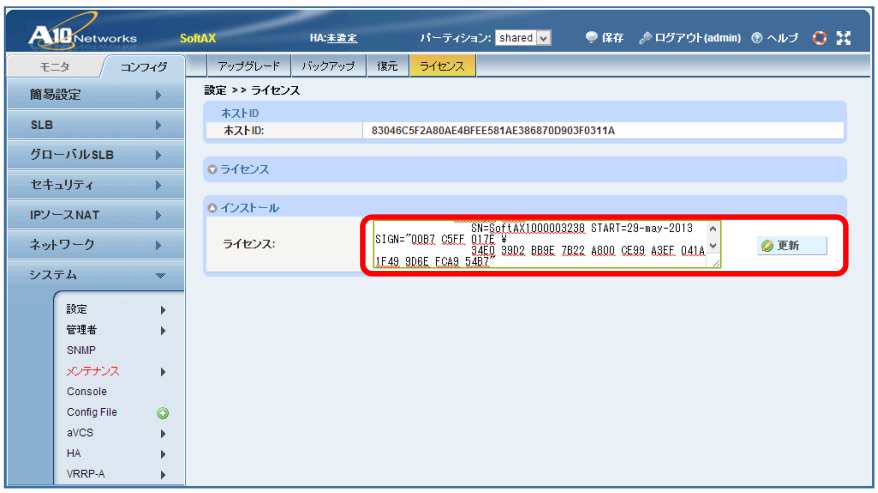
注意 : 本書の設定作業では、ブラウザとして FireFox を利用していますが、その他サポートされているブラウザ（Chrome 等）でも、同様なかたちでセキュリティの例外処理が必要となります。

ログインプロンプトが表示されたら、デフォルトの”ユーザ名” : “admin”、”パスワード” : “a10”でログインします。



コンフィグタブをクリックし、”メンテナンス” >> “ライセンス”を選択します。

取得したライセンス情報を貼り付けた後、更新をクリックし、ライセンスを適用します。



ライセンスが正しく適用されたことを確認します。

6.5　リバースプロキシ向け SoftAX の構成

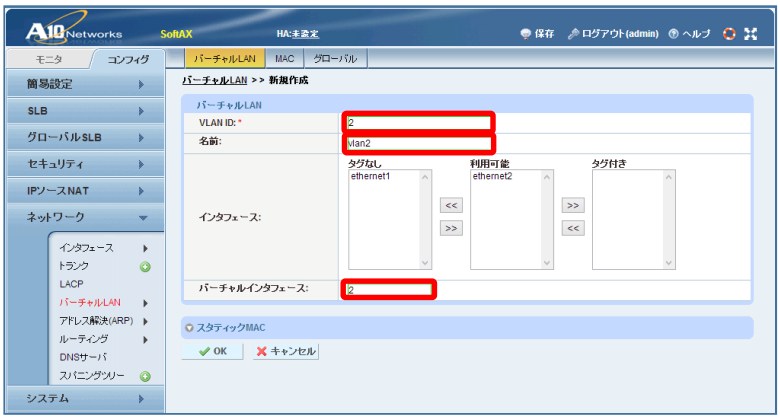
6.5.1 内部・外部ネットワークインターフェースの定義と有効化

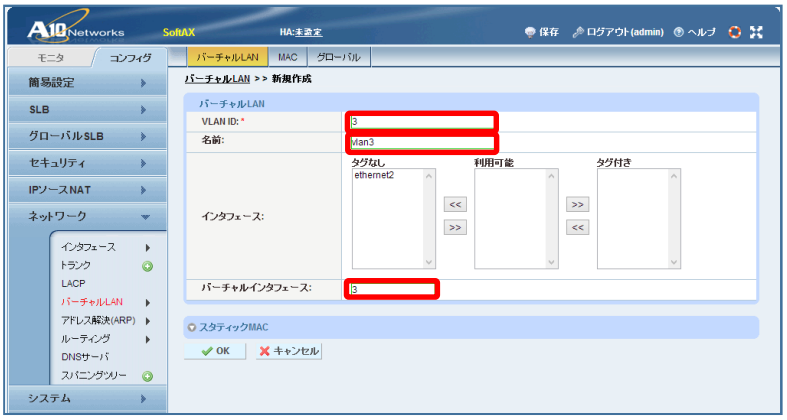
内部･外部ネットワークインターフェースの Ethernet1, Ethernet2 に VLAN を定義し、IP アドレスを設定します。

コンフィグタブの”ネットワーク” >> “バーチャル LAN”を選択し、“追加”でバーチャル LAN を定義します。

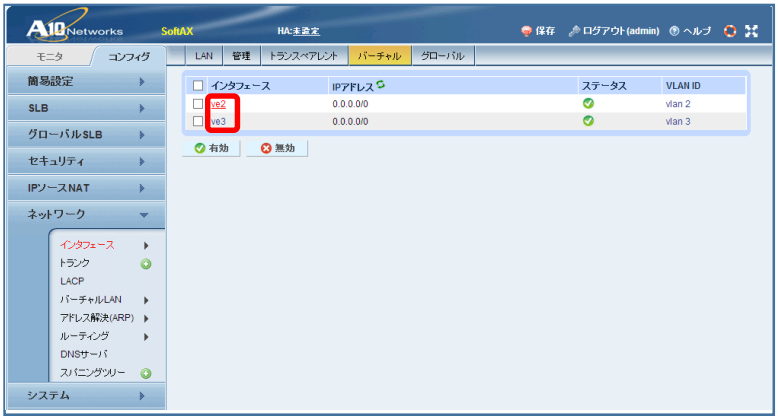
“VLAN ID”、”名前”、”バーチャルインターフェース”を入力し、VLAN を割り当てる”インターフェース”を”タグなし”もしくは”タグ付き”のいずれかに移動して完了します。タグ付きとはタグ VLAN の事で、AX/Thunder が接続するネットワークインターフェースがタグ VLAN で構成されていてポート VLAN を利用しない場合には、タグ付きを選択する必要があります。

通常のネットワーク構成であれば、ポート VLAN を利用することが多くタグなしで構成するケースがほとんどだと思われますが、適切な接続構成を実現するにあたり、必ず AX/Thunder が接続される先のネットワークの管理者に確認してください。



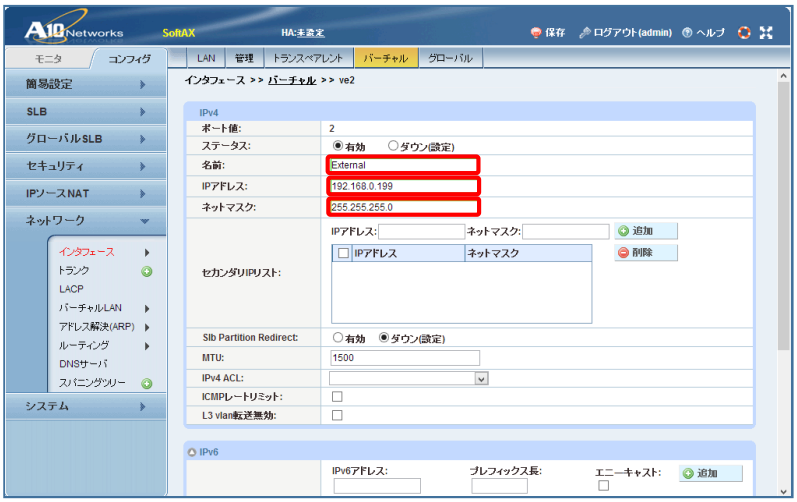


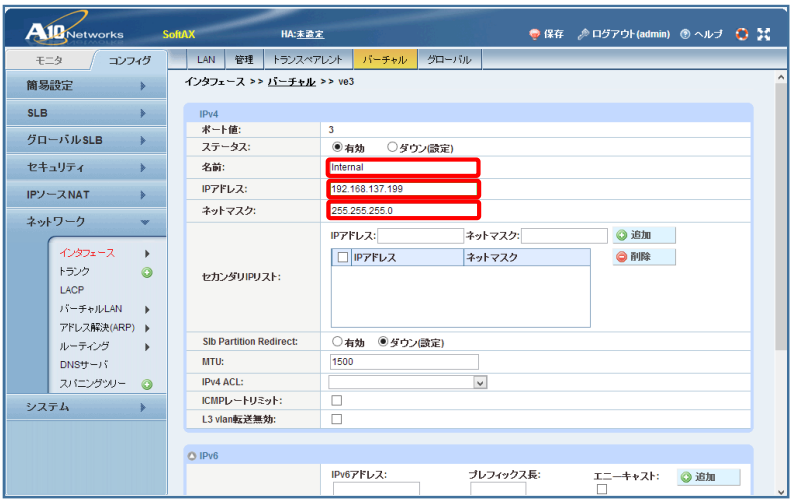
先に定義した VLAN インターフェースに IP アドレスを設定します。”ネットワーク” >> “インターフェース” >> “バーチャル”でリストを表示し、IP アドレスを設定する VLAN の”インターフェース”をクリックし、設定画面を開きます。



設定画面を開いたら、”名前”、”IP アドレス”、”サブネットマスク”に適切な値を入力し、”ステータス”が”有効”にチェックされていることを確認した上で、画面下部の”OK”ボタンをクリックして完了します。

本書のケースでは、vlan2 を外部公開用ネットワークとして、vlan3 を内部向けネットワークとして定義します。





注意：SoftAX のデータ用ネットワークインターフェース(ここでは、Ethernet1, 2)には IP アドレスを割り当てる必要があり、リバースプロキシを構成する場合には外部ネットワークインターフェースにグローバル IP アドレスを割り振る必要があります。つまりリバースプロキシ用に割り振る IP アドレスの他にグローバル IP アドレスがもう 1 つ必要となります。**(各インターフェースに割り振る IP アドレスと、実際にリバースプロキシで利用する IP アドレスは異なる必要があるといった制約のためです)**

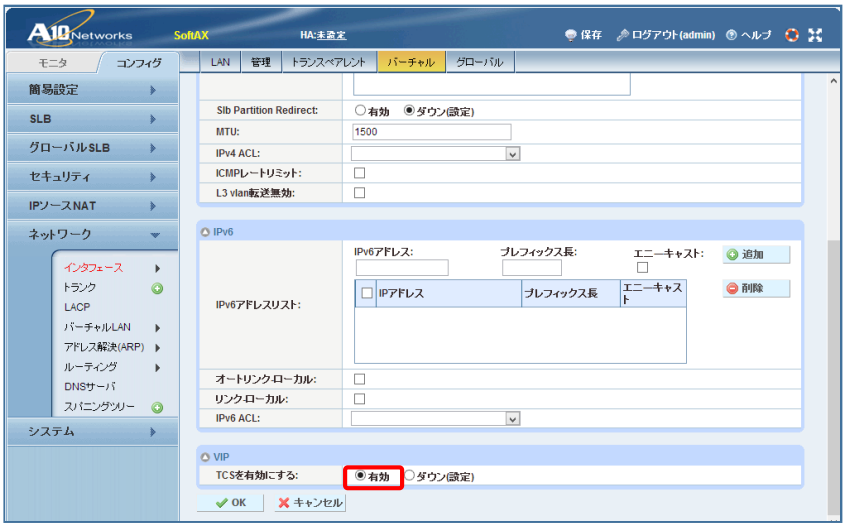
この問題を解消する方法として、AX/Thunder シリーズ(SoftAX を含む)の Promiscuous を利用し外部公開用ネットワークインターフェースには全く関係ないプライベート IP アドレスを割り振り、後のリバースプロキシの構成で

グローバル IP アドレスを仮想サーバーアドレスとして設定することで、使用するグローバル IP アドレスを最少化することが可能です。
但し、Promiscuous を利用する場合、実際のネットワークインターフェースに設定した IP アドレスが既存ネットワークに問題を引き起こさない様に十分留意する必要がありますのでご注意ください。

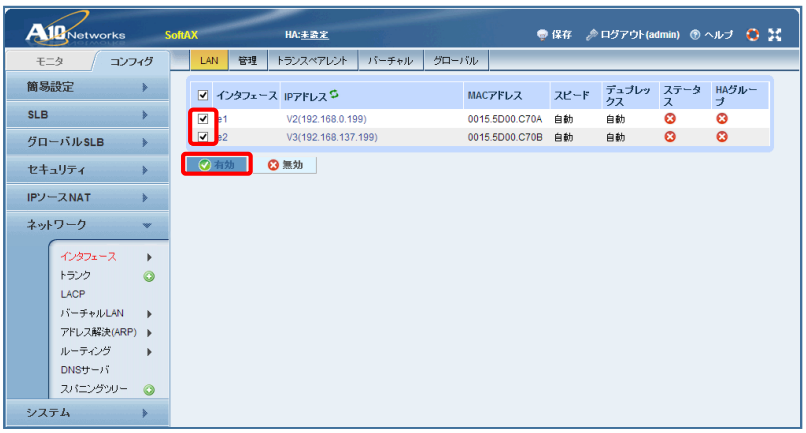
下記は、Promiscuous を有効化するための設定です。バーチャル LAN へ IP アドレスを設定する画面の下の方にある”VIP”を展開し、”TCS を有効にする:”で”有効”をチェックすることで Promiscuous は有効化されます。

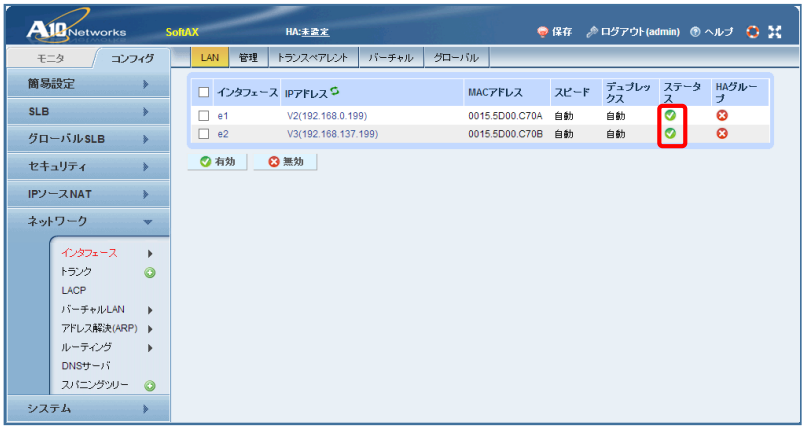
注意) Promiscuous の有効化は、IP アドレスの設定と同時に実施することができません。最初に IP アドレスの設定を実施し、その後再度インターフェースをクリックして設定画面を開き、Promiscuous の有効化を実施してください。

本書のケースでは、外部ネットワークインターフェース(vlan2)に割り振る IP アドレスを、Promiscuous を有効化し 192.168.0.199 という架空の IP アドレスにしています。



インターフェースを有効化するため、”インターフェース” >> “LAN”をクリックし、
有効化したいインターフェースをチェックして、インターフェースを有効化します。



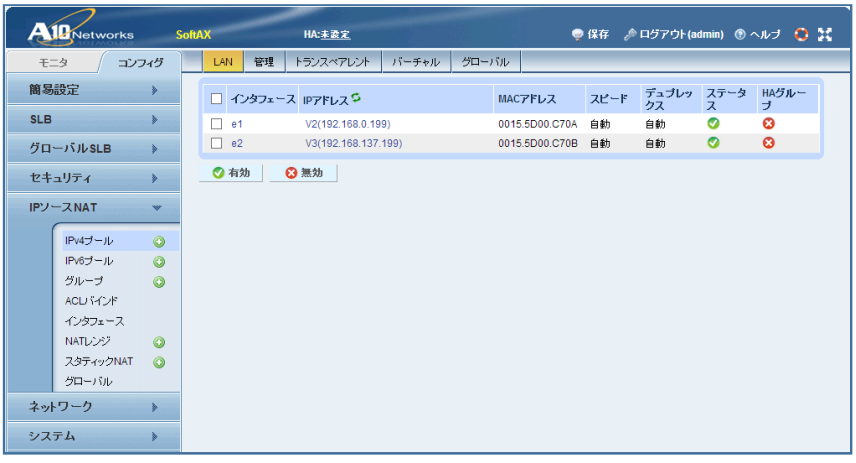


6.5.2 IP ソース NAT の定義

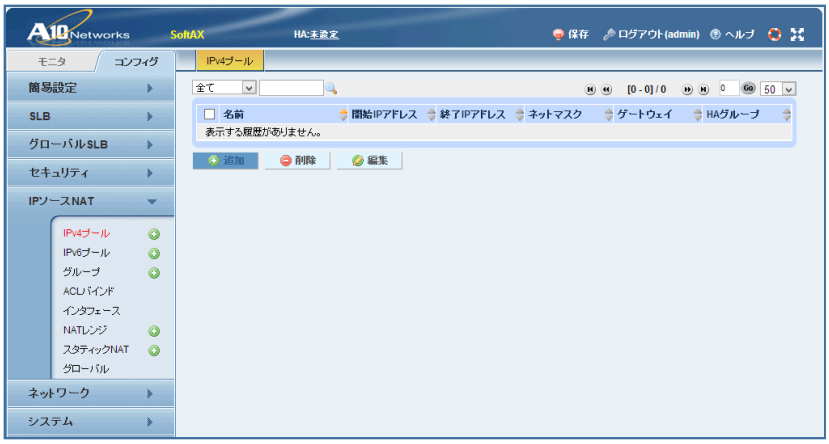
注意 ： リバースプロキシとして動作させるためには、外部(インターネット)からアクセスしてきたデバイスの送信元 IP アドレスを、AX/Thunder の内部インターフェースの IP アドレスに変更する必要があります。これを実現する方法として、本章で示している IP ソース NAT を定義し、6.5.8 章バーチャルサーバポートの設定画面上にあるソース NAT プールで選択する方法と、IP ソース NAT を定義せずバーチャルサーバポートの設定画面上にあるソース NAT プールで、”Auto”をチェックする方法の 2 つがあります。特に設定上問題なければ、後者の設定の方が容易です。

IP ソース NAT を定義します。AX/Thunder 経由で Lync のフロントエンドサーバー、Office Web Apps サーバーへのリモートクライアントからの Web 通信をリダイレクトするケースにおいて、ソース IP アドレスを変更しないと、Lync フロントエンドサーバーは返信先として AX/Thunder ではなく、リモートクライアントの IP アドレス(グローバル IP アドレス)に向けてセッションを確立しようとします(外部向け通信であるため、通常デフォルトゲートウェイ経由となるはずです)。そのため、AX/Thunder を経由した Web 通信が双方向で確立されず、リバースプロキシしての機能を実現することができない状態となります。この問題を解決するため、AX/Thunder 経由で Lync フロントエンドサーバー、Office Web Apps サーバーへ送信される Web 通信のソース IP アドレスを強制的に AX/Thunder の内部向けネットワークインターフェースの IP アドレスに書き換えて、Lync フロントエンドサーバー、Office Web Apps サーバーからの返信先を AX/Thunder の内部向けネットワークインターフェースにすることで対応します。

コンフィグタブの”IP ソース NAT IPv4 プール”をクリックします。



“追加”をクリックして、設定画面へ遷移します。



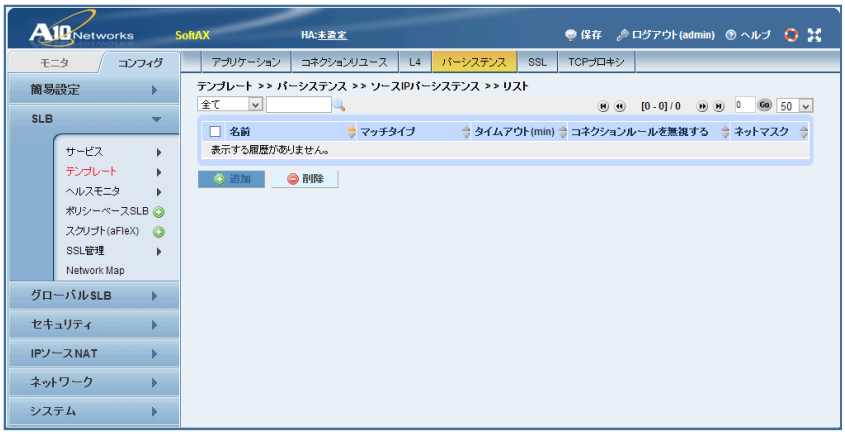
ここでは、“名前”、”開始 IP アドレス”、”終了 IP アドレス”と”ネットマスク”を入力し、開始 IP アドレスと終了 IP アドレスには、SoftAX の内部ネットワークインターフェースに割当てた IP アドレスを設定します。

6.5.3 ソース IP パーシステンス テンプレートの定義

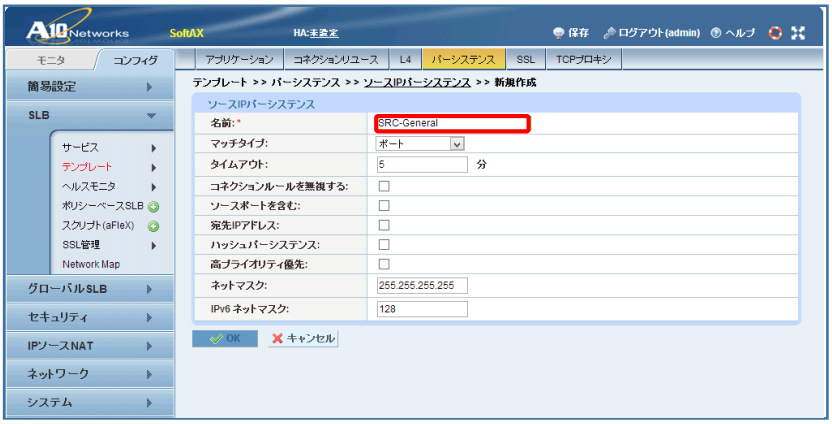
ソース IP パーシステンスは、送信元 IP アドレスが同一の通信を、同じサーバーリソースに割り振るためのオプションとなります。Lync や Office Web Apps が複数サーバーで構成されているような場合には、同一リモートクラアイントからのアクセスを同一サーバーに振り分けるために必要となります。

“SLB” >> “テンプレート” >> “パーシステンス” >> “ソース IP パーシステンス”をクリック

“追加”をクリックし、設定画面へ遷移します。



“名前”を入力、”マッチタイプ”で”ポート”を選択して、”OK”をクリックし終了します。



注意： マッチタイプには、この他 サーバーやサービスグループがあります。サーバーは指定された宛先 IP ソース毎に、送信元 IP ベースで振り分けます。つまり、宛先ポート番号が違う通信も、送信元 IP アドレス毎に同一サーバーにリダイレクトされます。ポートは、宛先ポート番号まで見て割り振りされますので、より細かいレベルでの分散が可能です。

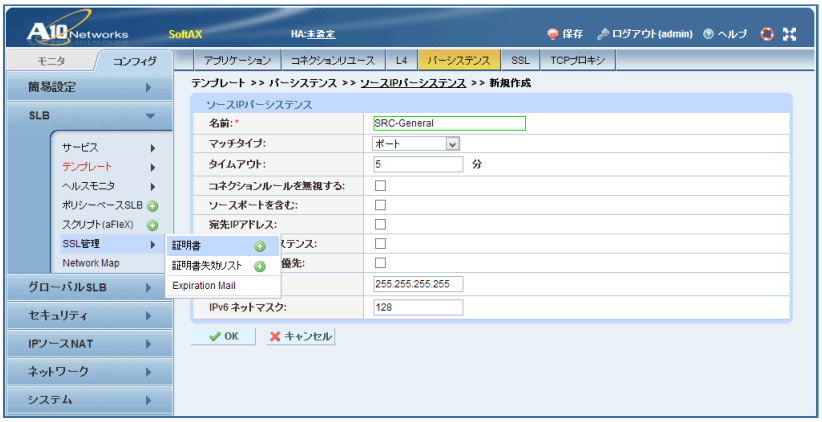
Lync のリバースプロキシ向け通信の宛先ポートは 443 しかないため、マッチタイプしてサーバーでも対応可能ですが、本書のケースではポートで設定しています。

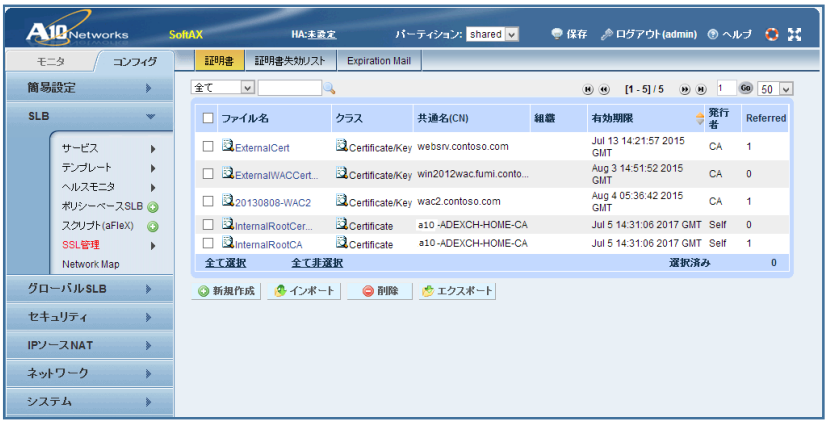
6.5.4 証明書インポート

本書の冒頭部分で作成した証明書を SoftAX にインポートします。本書の構成では、以下の証明書を使用します。

1. Lync フロントエンドサーバー外部公開 Web サーバー証明書 (秘密鍵付き)
2. Office Web Apps サーバー外部公開 Web サーバー証明書(秘密鍵付き)
3. 内部認証局(CA)のルート証明書

コンフィグタブの、”SLB” >> “SSL 管理” >> “証明書”をクリック

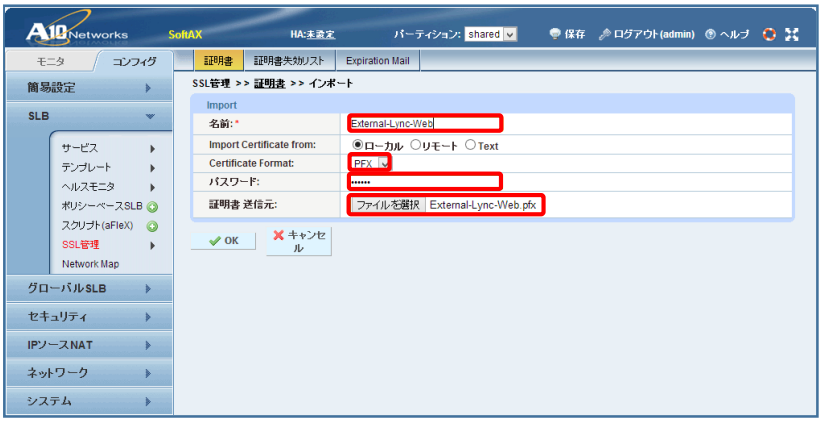




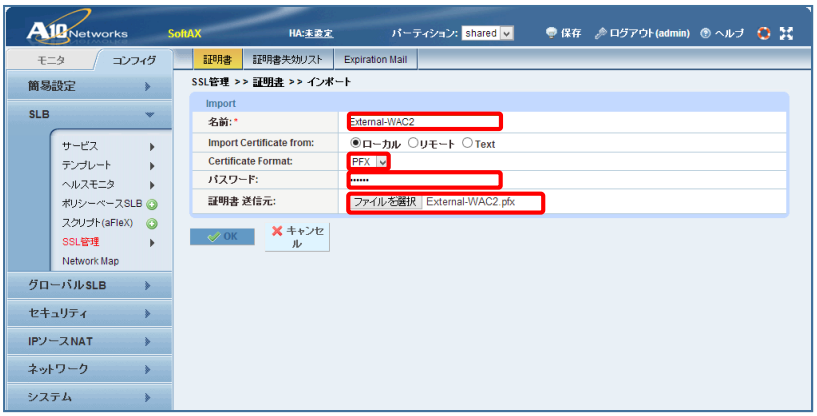
インポートされている証明書リストが表示されます。もし、新規で SoftAX を立ち上げた場合、こちらのリストは空となります。
インポートをクリックし、画面に従って先に記した 3 種類の証明書をインポートします。

“名前”は後の証明書を割り当てる際に使用しますので、判り易い名前を入力します。”
証明書 送信元:”でインポートする証明書を選択し、”パスワード:”で証明書(秘密鍵)を
エクスポートする際に設定したパスワードを入力して、”OK”をクリックします。
ルート証明書は鍵情報を含んでいないため、インポート時のパスワード入力は必要あ
りません。

- Lync フロントエンドサーバー外部公開 Web サーバー証明書 (秘密鍵付き)

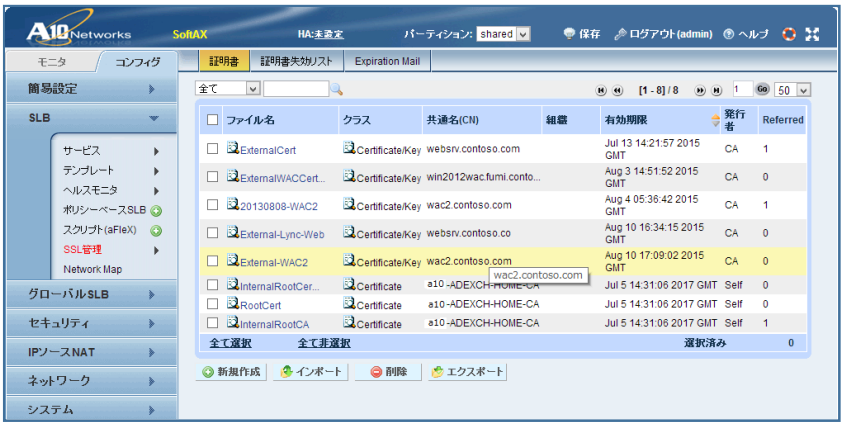


- Office Web Apps サーバー外部公開 Web サーバー証明書 (秘密鍵付き)



- 内部認証局(CA)のルート証明書

証明書がすべて正常にインポートされていることを確認して終了します。



6.5.5 SSL テンプレートの設定

インポートした証明書を利用して、SSL テンプレートを作成します。SSL テンプレートにはサーバーとクライアントの区別があり、以下の様に使い分けます。

- ✧ クライアント SSL テンプレートは、AX/Thunder がリモートクライアントからの通信を、Lync フロントエンドや Office Web Apps の Web サーバーとして中継するために利用されます。
- ✧ サーバーSSL テンプレートは、AX/Thunder が Lync クライアントとして、Lync フロントエンドや Office Web Apps のサーバーと通信をするために利用されます。

本書のケースでは、クライアント SSL テンプレートとして、Lync フロントエンドサーバー用と、Office Web Apps サーバー用の 2 つを作成し、サーバーSSL テンプレートを 1 つ定義します。
クライアント SSL テンプレートが 2 つ必要なのは、Lync フロントエンドサーバー外部公開 Web サーバー証明書と Office Web Apps サーバー外部公開 Web サーバー証明書が独立しているためです。

注意 ： 各クライアント SSL テンプレートに割り当てられる証明書は 1 つだけです。

本書のケースでは、サーバーSSL が利用する内部認証局(CA)のルート証明書は、Lync フロントサーバー、Office Web Apps サーバーで共通のため、サーバーSSL テンプレートは 1 つで十分です。

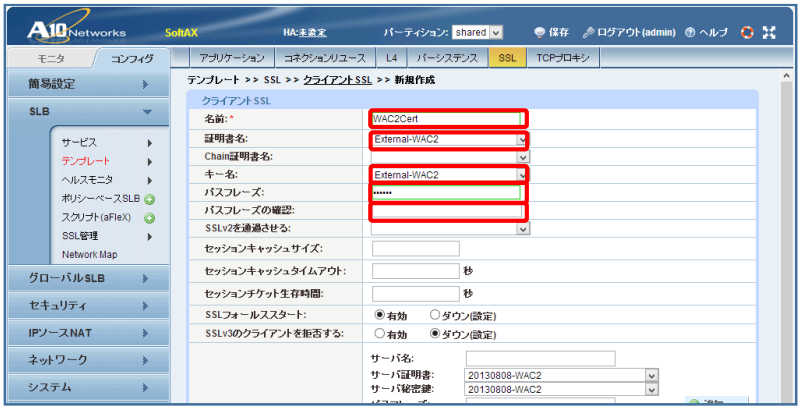
“SLB” >> “テンプレート” >> “SSL” >> “クライアント SSL”をクリックします。

追加をクリックし、設定画面へ遷移します。

Lync フロントエンドサーバー外部公開 URL 向けにクライアント SSL テンプレートを作成します。

“名前”を入力し、”証明書名”と”キー名”で先ほどインポートした Lync フロントエンドサーバー外部公開 Web サーバー証明書を選択し、”パスフレーズ”に証明書(秘密鍵)エクスポート時に設定したパスワードを入力し、画面下部の”OK”をクリックして終了します。

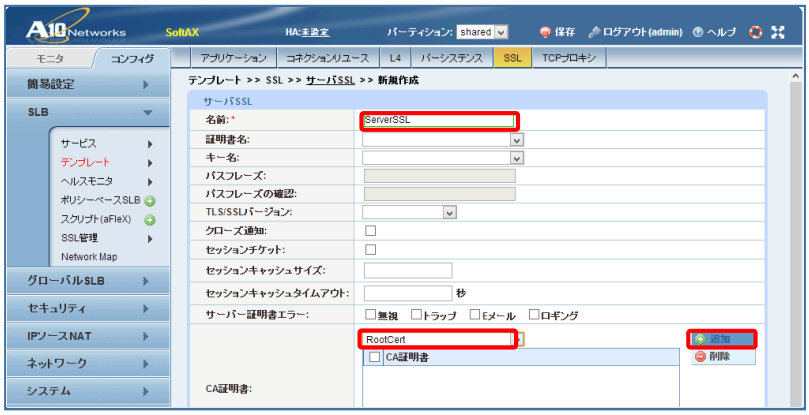
同様の設定で Office Web Apps サーバー外部公開 URL 向けのクライアント SSL テンプレートを、Office Web Apps 外部公開 Web サーバー証明書を利用して作成します。

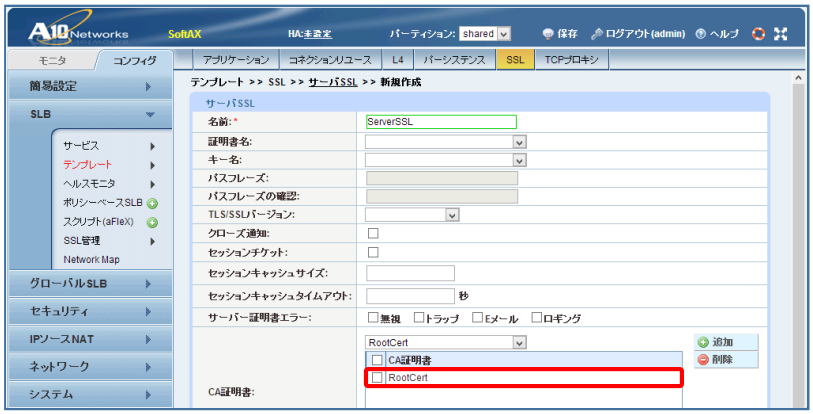


サーバーSSL テンプレートを構成します。

“SLB” >> “テンプレート” >> “SSL” >> “サーバーSSL”でリスト画面に遷移し、”追加”をクリックします。

“名前”を入力し、”CA 証明書”に、先ほどインポートした内部認証局(CA)のルート証明書を選択し、”追加”をクリックして追加し、完了します。





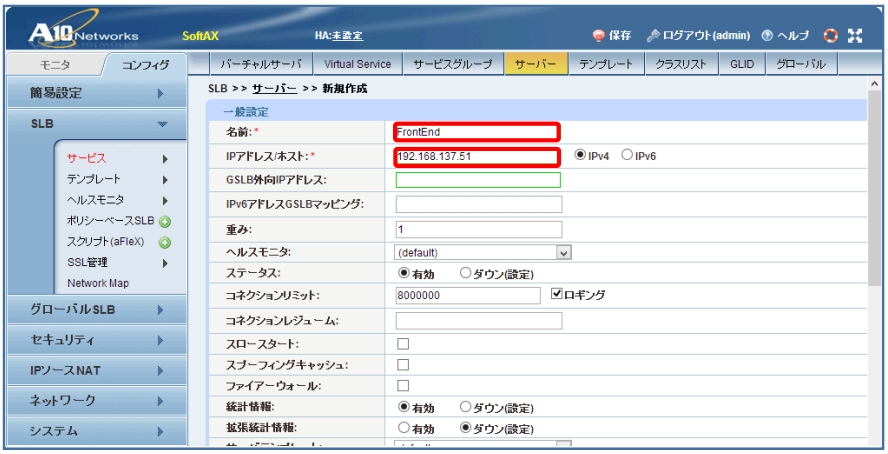
6.5.6 サーバーの設定

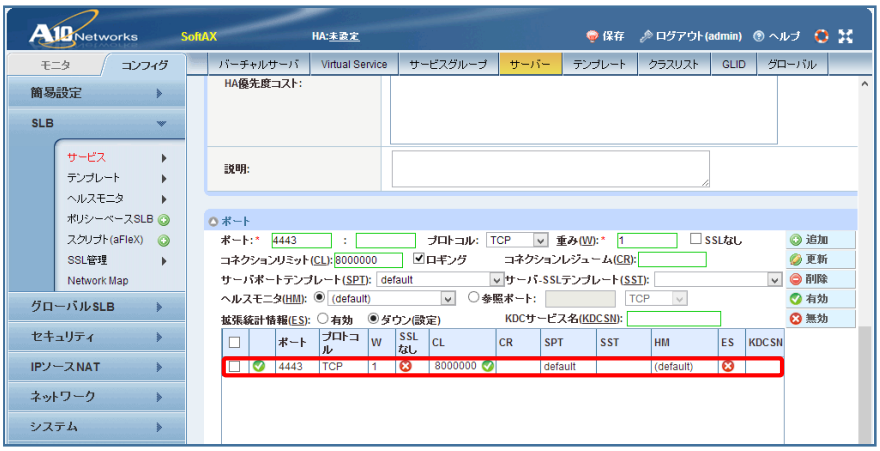
Lync フロントエンドサーバーと Office Web Apps サーバーの IP アドレスと通信ポートをサーバーとして定義します。

“SLB” >> “サービス” >> “サーバー” でメニューを展開し、”追加”をクリックして設定を行います。

- Lync フロントエンドサーバー

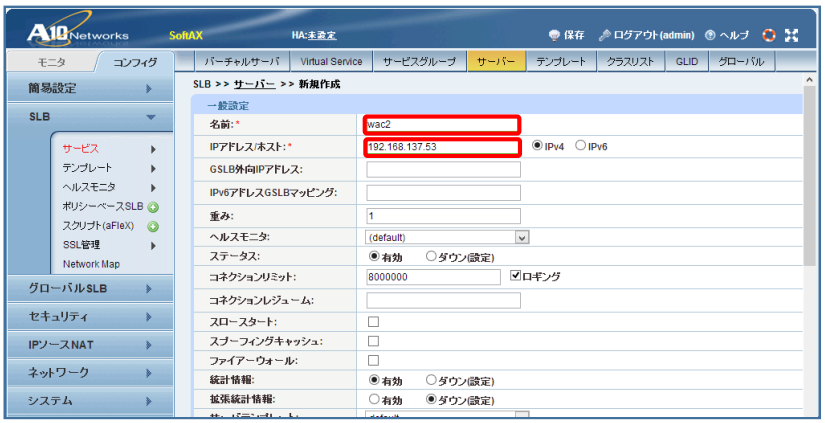
  “名前”、”Lync フロントエンドサーバーの IP アドレス”を入力し、”ポート番号 4443” を追加して終了します。

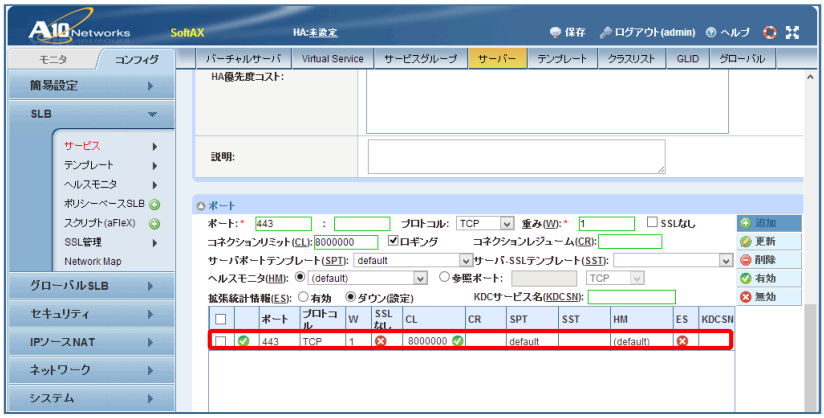




- Office Web Apps サーバー

  Lync フロントエンドサーバーと同様に、”名前”、”Office Web Apps サーバーの IP アドレス”、”ポート番号 443”を追加して終了します。

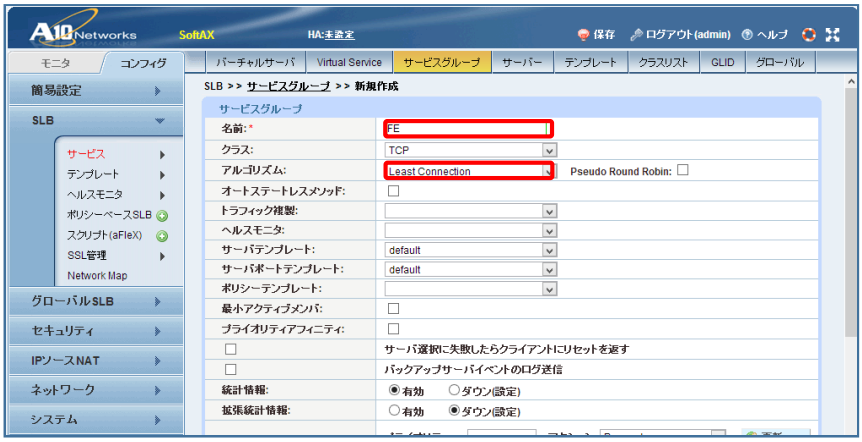


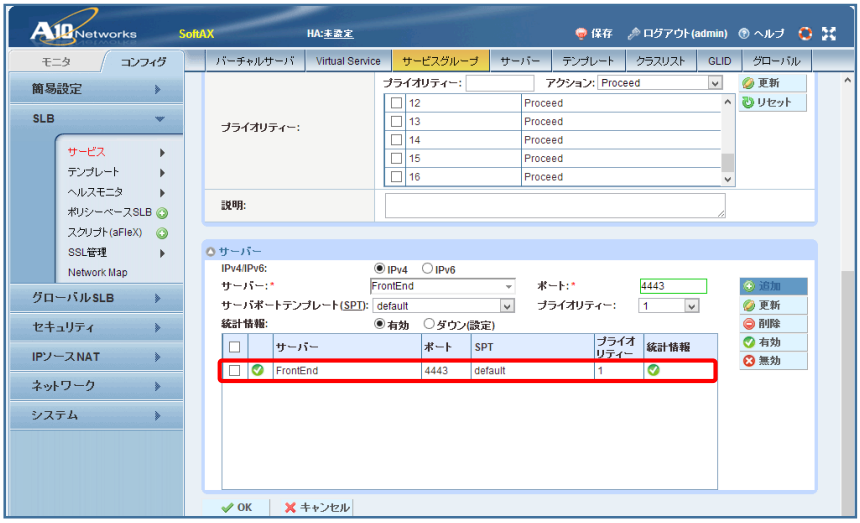


6.5.7 サービスグループの設定

“サービスグループ”を選択し、”追加”をクリックして、Lync フロントエンドと Office Web Apps 向けのサービスグループを各々作成します。

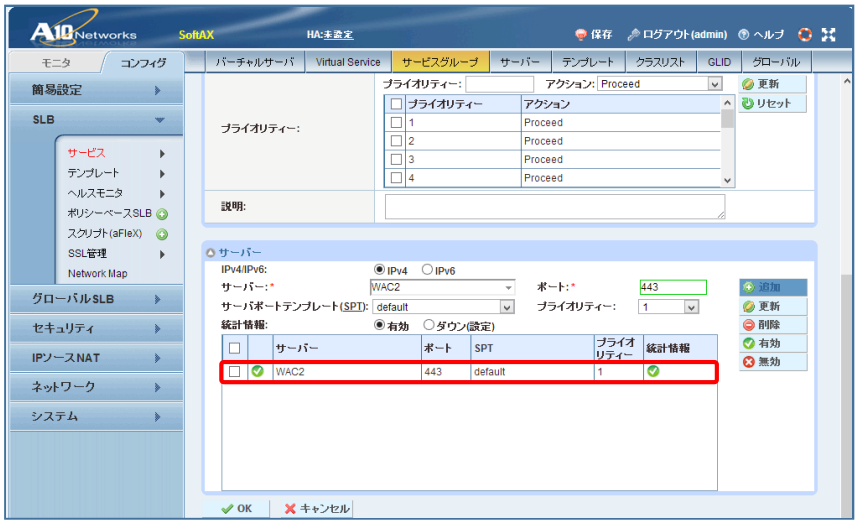
- Lync フロントエンド向けサービスグループ
  “名前”を入力し、クラスで”TCP”を選択します。アルゴリズムは、今回接続数が最小のサーバーに優先的に接続する”Least Connection”を選択し、サーバーとして先ほど定義した”FrontEnd”を指定して、”ポート 4443”のレコードを追加します。



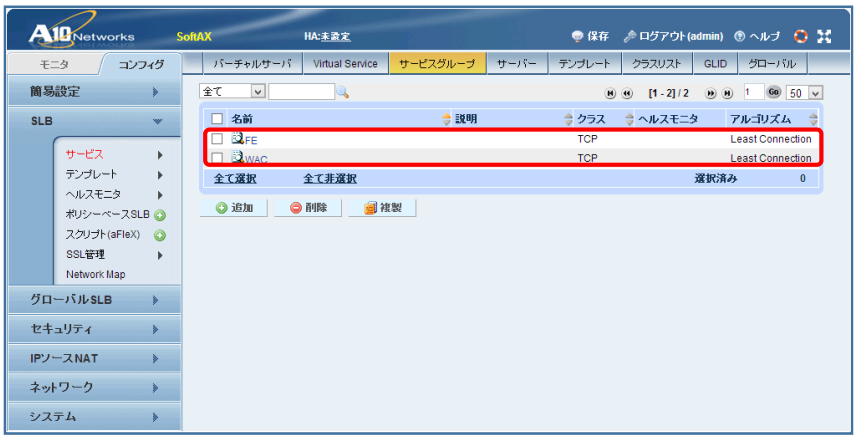


- Office Web Apps 向けサービスグループ

  基本的に Lync フロントエンドサーバーと同様ですが、サーバーに”WAC2”を指定して、”ポート 443”のレコードを追加する点が異なります。



Lync フロントエンドサーバー向け、Office Web Apps サーバー向けのサービスグループが定義されたことを確認します。



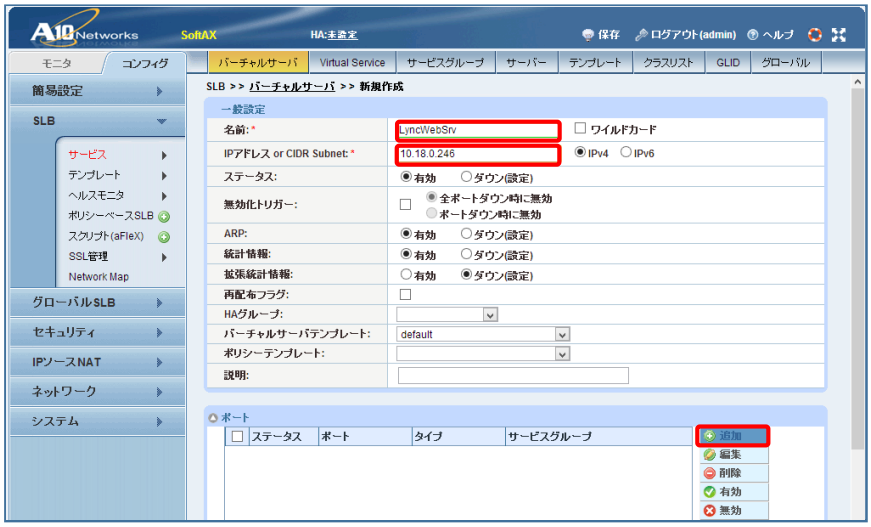
6.5.8 バーチャルサーバとバーチャルサーバポートの設定

バーチャルサーバを定義します。”バーチャルサーバ”を選択し、”追加”をクリックします。

- Lync フロントエンドサーバー外部公開 URL 向け設定

  名前を入力し、Lync フロントエンドサーバー外部公開 IP アドレスを入力します。

  ポートの”追加”をクリックし、バーチャルサーバポート設定画面へ遷移します。



バーチャルサーバポート設定画面で、以下の内容を設定します。

タイプ ：HTTPS

ポート ：443 (リモートクライアントからの接続ポート)

サービスグループ ： FE

ラストホップを使用する ： チェック

(Promiscuous を利用しグローバル IP アドレス数を極少化する場合必須です。)

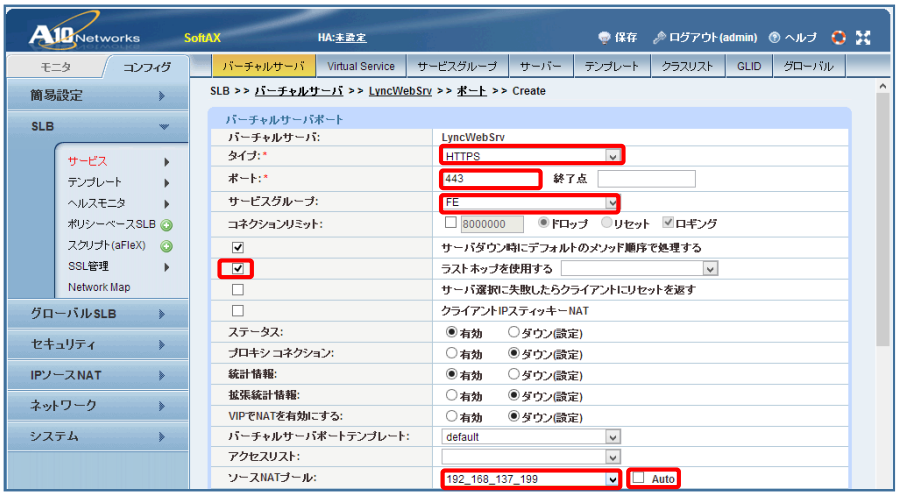
ソース NAT プール ：192_168_137_199 もしくは Auto

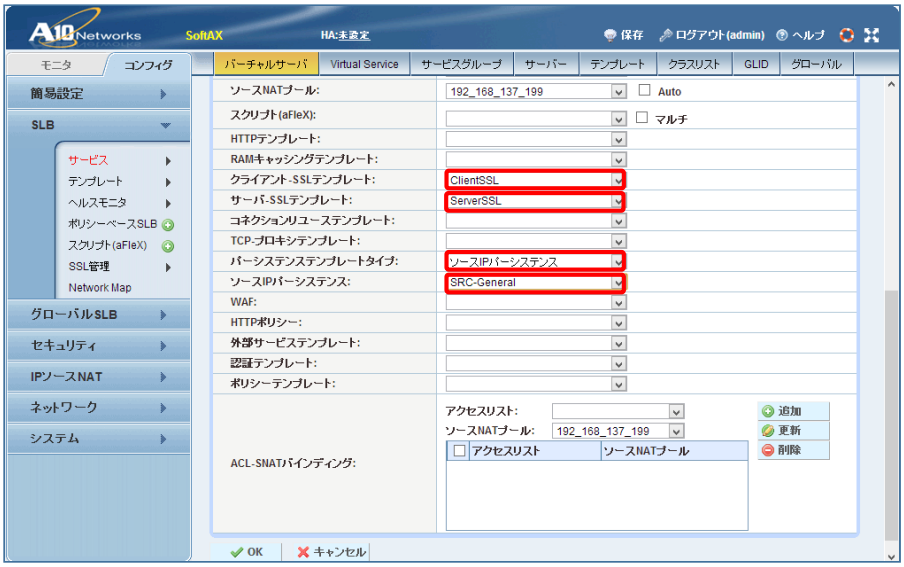
クライアント-SSL テンプレート ：ClientSSL

サーバ-SSL テンプレート ：ServerSSL

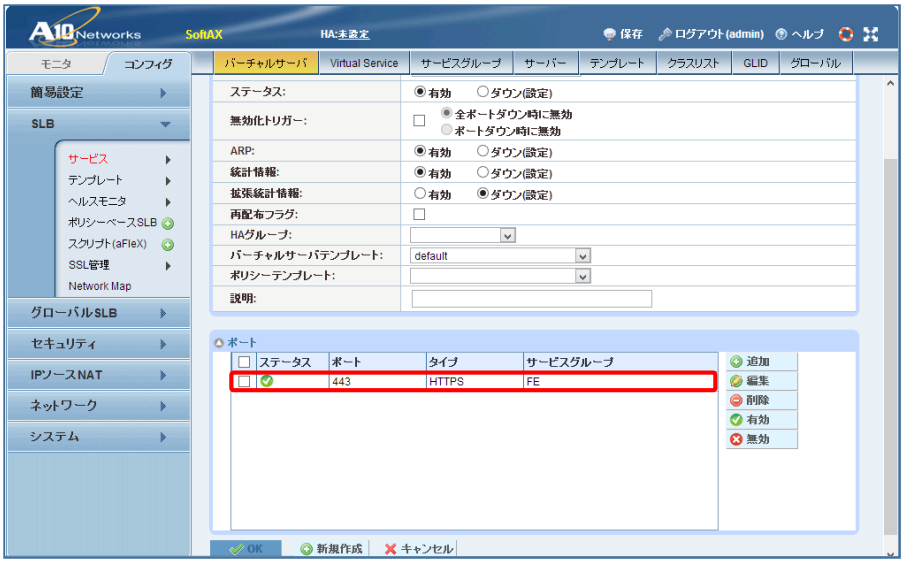
パーシステンス テンプレートタイプ ： ソース IP パーシステンス

ソース IP パーシステンス ：SRC_General



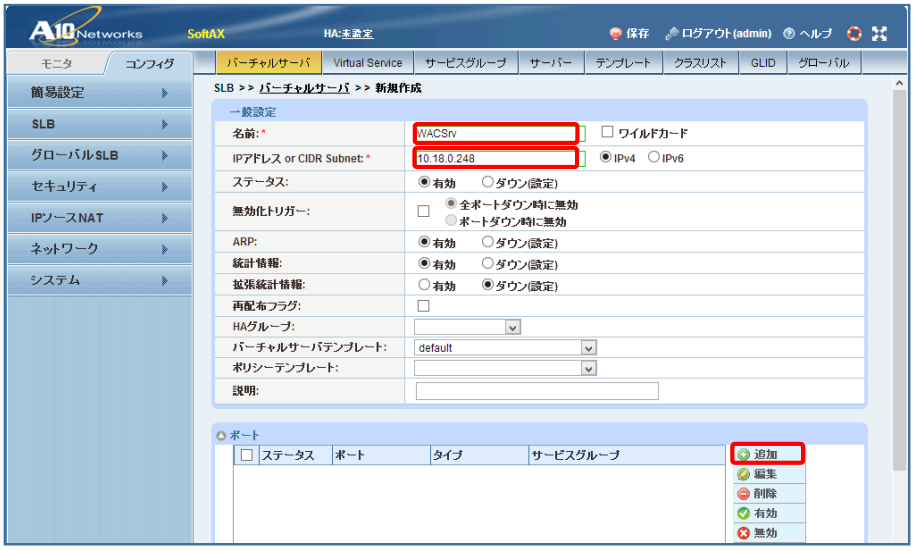


バーチャルサーバポート設定画面を”OK”で終了すると、再度バーチャルサーバの設定画面に戻るため、ポート設定が反映されていることを確認した上で、”OK”をクリックし設定を完了します。



- Office Web Apps サーバー公開用 URL 向け設定

  名前を入力して、Office Web Apps サーバー外部公開用 IP アドレスを入力し、残りの設定はデフォルトのままで、ポートの”追加”をクリックし、バーチャルサーバポート設定画面へ遷移します。



バーチャルサーバポート設定画面で、以下の内容を設定します。

タイプ ：HTTPS

ポート ：443 (リモートクライアントからの接続ポート)

サービスグループ ：WAC

ラストホップを使用する ： チェック

(Promiscuous を利用しグローバル IP アドレス数を極少化する場合必須です。)

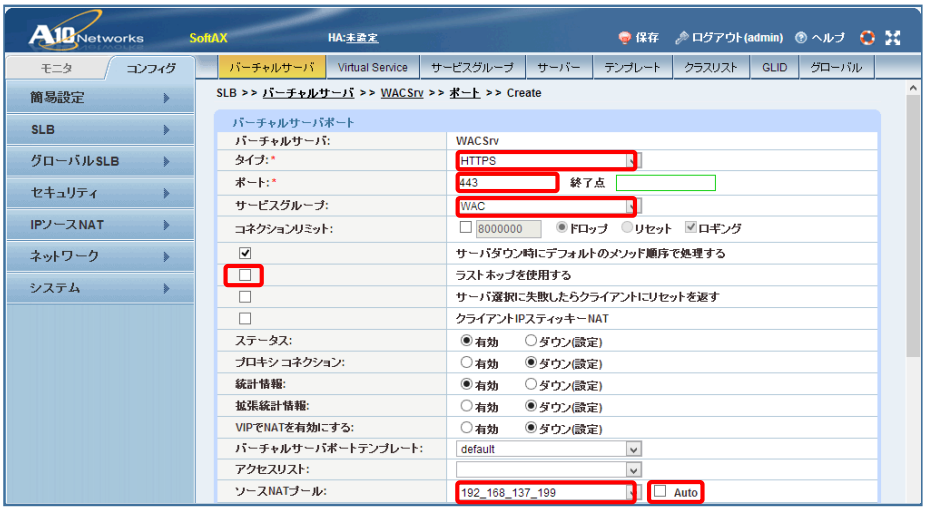
ソース NAT プール ：192_168_137_199 もしくは Auto

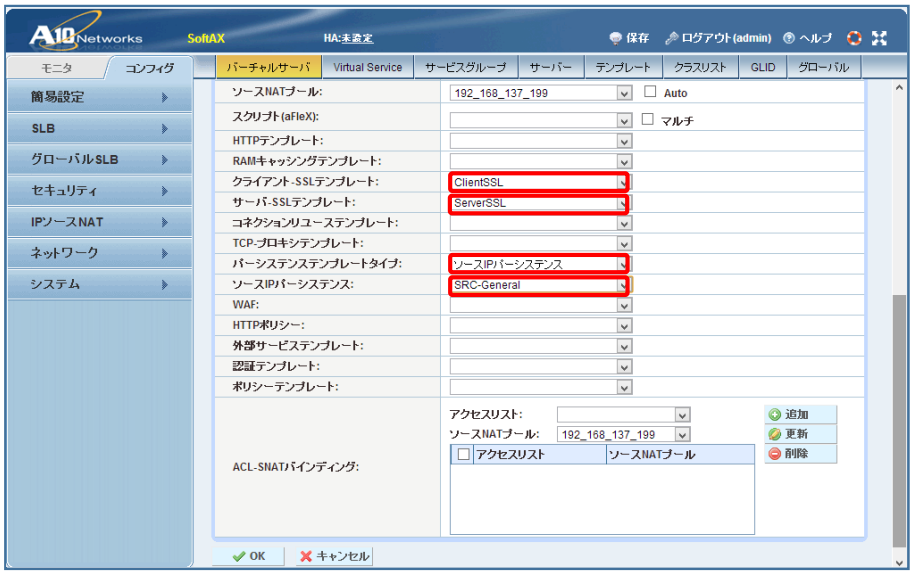
クライアント-SSL テンプレート ：WAC2Cert

サーバ-SSL テンプレート ：ServerSSL

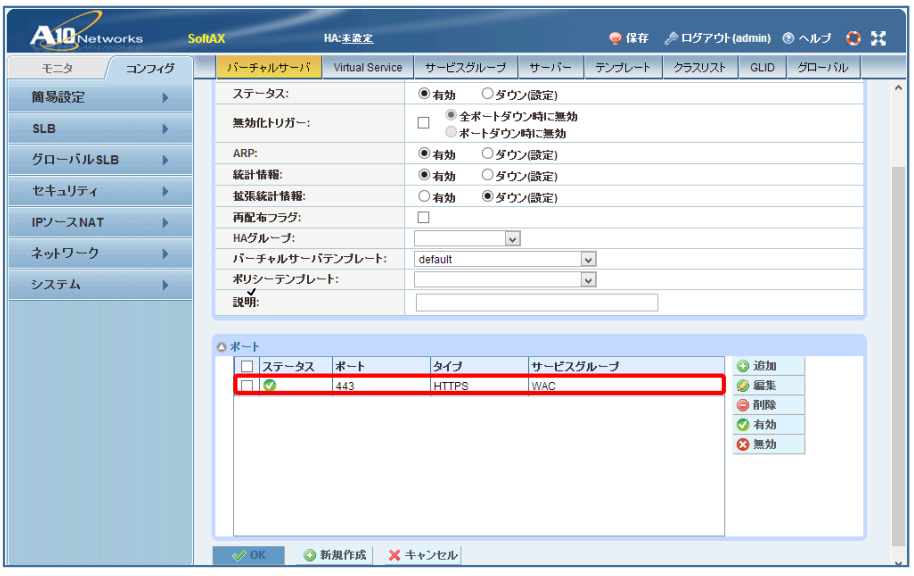
パーシステンステンプレートタイプ ： ソース IP パーシステンス

ソース IP パーシステンス ：SRC_General





バーチャルサーバポート設定画面を”OK”で終了すると、再度バーチャルサーバの設定画面に戻るため、ポート設定が反映されていることを確認した上で、”OK”をクリックし設定を完了します。

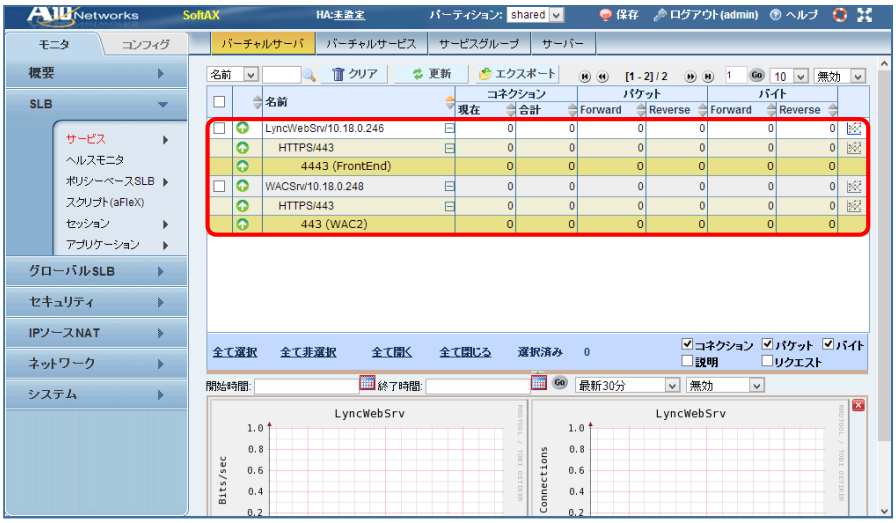


バーチャルサーバとして、Lync と Office Web Apps 向けの設定が反映されていることを確認します。

以上で、SoftAX を利用した Lync 向けリバースプロキシの構成は完了です。
最後に、保存ボタンをクリックし設定内容を保存します。

6.5.9 設定データの動作確認

Web 設定画面のモニタタブへ移り、”SLB” >> “サービス” >> “バーチャルサーバ”を選択後、画面中央の”全てを開く”をクリックして、現在のサービス並びにサーバーの状態を確認します。下記のように各サーバー名横のアイコンがグリーンで表示されていれば、AX/Thunder からそれぞれのサーバーのサービスに問題なく到達できていることとなります。

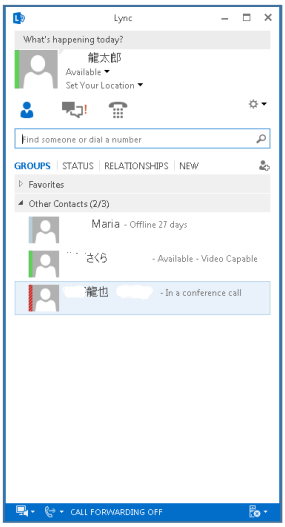


7 動作確認結果

リバースプロキシ経由で Lync フロントエンドサーバーと Office Web Apps サーバーを利用するシナリオとして、社内ネットワークの Lync 2013、社外の Lync 2013 と Lync モバイル 2013 の三者で Web 会議を実施し、パワーポイントを共有するテストシナリオで AX/Thunder シリーズのリバースプロキシとしての動作を確認します。

7.1 Lync 2013 リモートクライアント(社外)のサイン後の画面

Lync 2013 (Client02) – リバースプロキシ経由のアドレス帳等のダウンロード



Lync モバイル for iPAD (Client03) – リバースプロキシ経由でサインインします。

7.2　会議開催時の画面

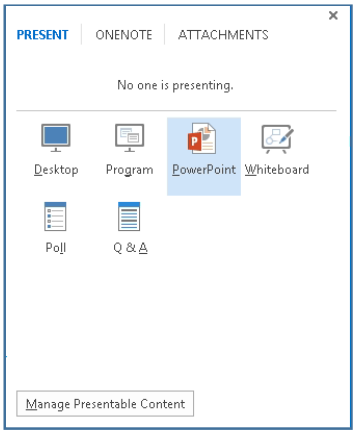
社内ネットワーク内の Lync 2013 (Client01)で、今すぐ会議を実行

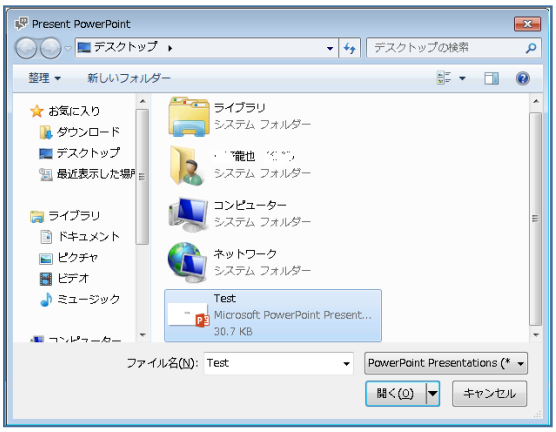
Lync 2013 (Client01)

7.3　資料共有開始時の画面

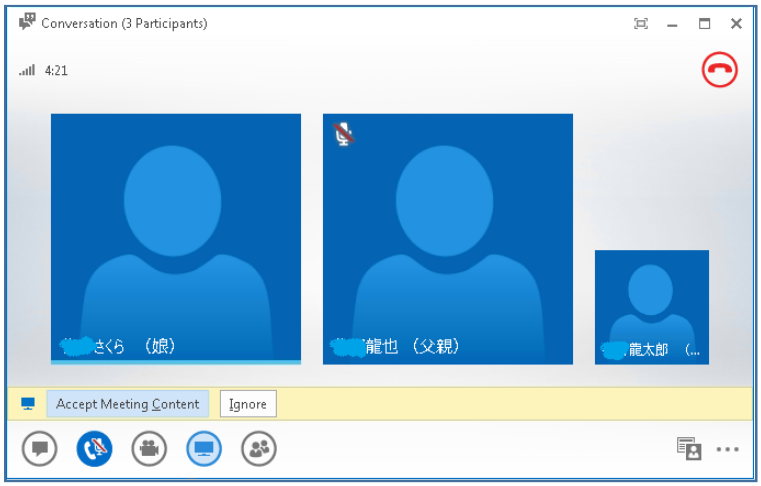
社内ネットワーク内の Lync 2013 (Client01)でパワーポイント資料の共有を実行

Lync 2013 (Client01)

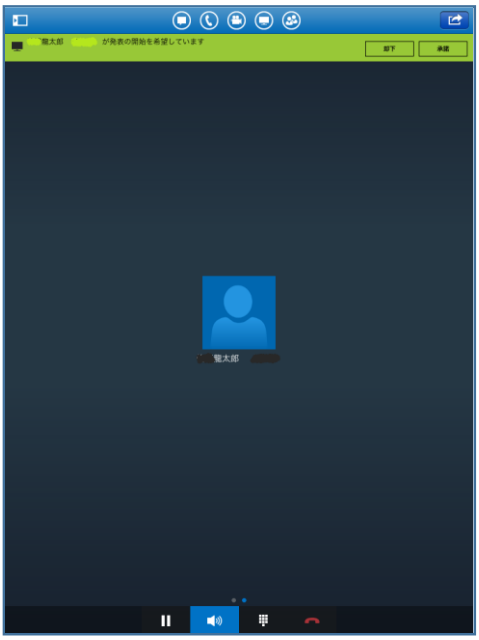




Lync 2013 (Client02)



Lync モバイル 2013 for iPad (Client03)

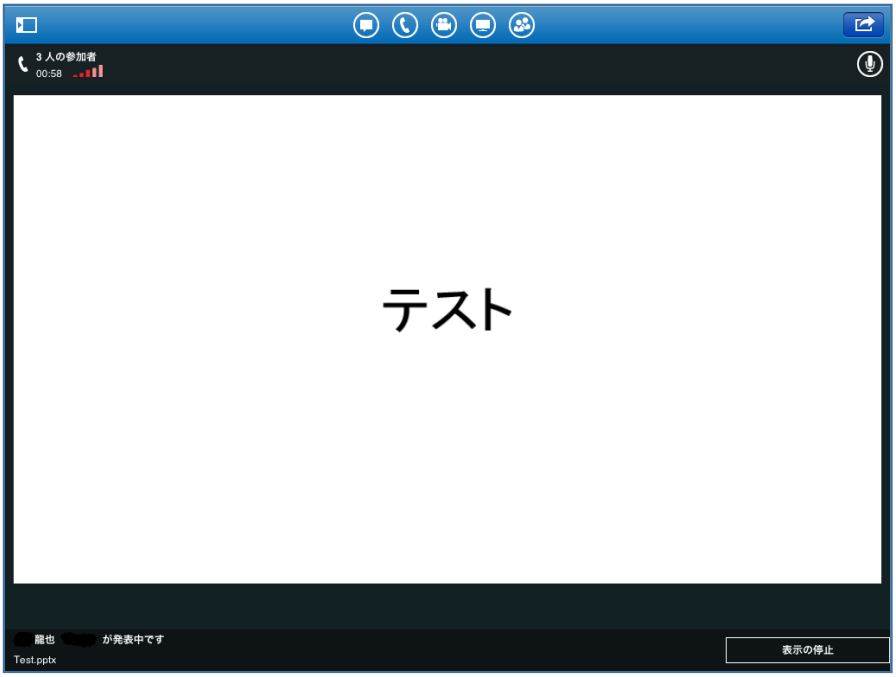


7.4　資料共有時の画面

Lync 2013 (Client01) –発表者

Lync 2013 (Client02) – リバースプロキシ – Office Web Apps サーバー経由でパワーポイント資料共有

Lync モバイル 2013 for iPAD (Client03)



8 最後に

動作確認テストでは、Lync モバイル 2013 クライアントと外部ネットワーク(仮想インターネット)上の Lync 2013 を利用し、AX/Thunder シリーズ(SoftAX)が Lync アーキテクチャーのリバースプロキシとして動作することを以下の項目で確認しています。

- 社外 Lync 2013 からのサインイン時に利用する、Lyncdiscover.contoso.com 経由のアクセス
- 社外 Lync 2013 へのアドレス帳(GalContact)のダウンロード
- 社外 Lync 2013 からのスケジュール会議 URL 経由での参加
- 社外 PC からの Web スケジューラーへのアクセス

9 Appendix - SoftAX 設定データ情報 (running-config)

```
!version 2.7.1-P2, build 57 (Aug-03-2013,07:21)
!
hostname SoftAX
!
clock timezone Asia/Tokyo nodst
!
vlan 2
  untagged ethernet 1
  router-interface ve 2
!
vlan 3
  untagged ethernet 2
  router-interface ve 3
!

interface management
  ip address 192.168.10.69 255.255.255.0
!
interface ethernet 1
  name "e1"
!
interface ethernet 2
  name "e2"
!
interface ve 2
  ip address 192.168.0.199 255.255.255.0
  ip allow-promiscuous-vip
  name "vlan2"
!
interface ve 3
  ip address 192.168.137.199 255.255.255.0
  name "vlan3"
!
ip nat pool 192_168_137_199 192.168.137.199 192.168.137.199 netmask /24
!
slb template server-ssl ServerSSL
     ca-cert RootCert
!
!
slb server FrontEnd 192.168.137.51
     port 4443    tcp
!
slb server WAC2 192.168.137.53
     port 443    tcp
!
slb service-group FE tcp
       method least-connection
       member FrontEnd:4443
!


slb service-group WAC tcp
       method least-connection
       member WAC2:443
!
```

```
    slb template client-ssl ClientSSL
        cert External-Lync-Web
        key External-Lync-Web pass-phrase encrypted
    /+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
    !
    slb template client-ssl WAC2Cert
        cert External-WAC2
        key External-WAC2 pass-phrase encrypted
    /+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
    !
    slb template persist source-ip SRC-General
        incl-sport
    !
    slb virtual-server LyncWebSrv 10.18.0.246
        port 443    https
            name _10.18.0.246_HTTPS_443
            source-nat pool 192_168_137_199
            service-group FE
            use-rcv-hop-for-resp
            template client-ssl c-ssl
            template server-ssl s-ssl
            template persist source-ip SRC-General
    !
    slb virtual-server WACSrv 10.18.0.248
        port 443    https
            name _10.18.0.248_HTTPS_443
            source-nat pool 192_168_137_199
            access-list 102
            service-group WAC
            use-rcv-hop-for-resp
            template client-ssl wac-cert
            template server-ssl s-ssl
            template persist source-ip SRC-General
    !
end
```